

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

رقم التسجيل: 94/11674

الرقم التسلسلي: 186911

العسكرة الرقمية وتأثيرها على أمن الدول

دراسة حالة: التنافس الرقمي الروسي-الأمريكي

مذكرة مكملة للحصول على درجة الماستر في العلوم السياسية

تخصص: علاقات دولية ودراسات أمنية

إعداد الطالبة:

صالحي فاطمة

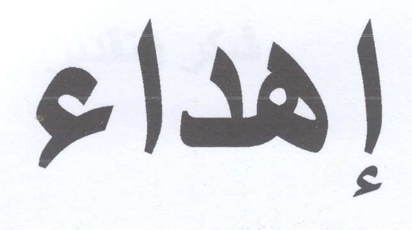
إشراف الأستاذة:

لفحل ليندة

أعضاء لجنة المناقشة:

الاسم واللقب	الدرجة العلمية	الجامعة	الصفة
عبد الغني دندان	أستاذ مساعد أ	8 ماي 1945 – قالمة	رئيسا
ليندة لفحل	أستاذ مساعد أ	8 ماي 1945 – قالمة	مشرفا ومقررا
اليامين بن سعدون	أستاذ مساعد أ	8 ماي 1945 – قالمة	عضوا ممتحنا

السنة الجامعية 2017 /2018



إلى أمي بكل حب و امتنان

إلى زوجي المحب الذي كان خير سند ومعين

الأطفالي الأعزاء : أيمن ...لينة...نورهان....نادين حلا

إلى أسرتي الكريمة التي شاركها هذا الجهد المتواضع وقتي

و

اهتمامي و التي احتضنت هذا العمل بكل رعاية و تفهم

أقرن،

اهدائي بعميق اعتذاري

شكر وتقدير

يشرفني أن أتقدم بشكري لكل من ساهم في المساعدة هذا البحث المتواضع وأخص بالذكر الأسرة العلمية و الأكاديمية بقسم العلوم السياسية والعلاقات الدولية لجامعة قالمة 1945
الأفاضل الذين لم يبخلوا بجهدهم على تكويننا خير تكوين،كما أتوجه بالشكر للجنة المناقشة لقبولها مناقشة البحث المقدم و التفضل بملاحظاتها القيمة التي نتشرف بتلقيها و العمل على أساسها.

- أتقدم بجزيل شكري لمشرفة البحث الأستاذة لفحل لينده على تأطيرها المشرف و صبرها الملحوظ و توجيهاتها البناءة التي رافقت سطور هذه الدراسة .

- أخص بالتقدير و الاحترام الأستاذة بلخير آسيا و التي كانت خير موجه ومعين وقد ألهمتني رؤيتها الثاقبة و حماسها الأخاذ لاختيار الموضوع و الاستمرار في البحث فيه.

- لا أنسى أن أوجه كل امتناني و اعترافي بالجميل مع شديد الفخر و الاعتزاز للغالية لمياء والتي لولا تشجيعها الدائم لما كان ممكنا استكمال هذه الدراسة بأي شكل من الأشكال، تحية لإخلاصها و تفانيها في خدمة العلم و تسهيل مهمة الطلبة .

خطة البحث

الفصل الأول: تحديد المجال،ضبط مفاهيمي و تأصيل نظري للدراسة

المبحث الأول: تحديد المجال:الانتقال من الجغرافيا للفضاء الرقمي

المطلب الأول: تعريف الفضاء الرقمي

الفرع الأول:مكونات الفضاء الرقمي

الفرع الثاني: خصائص الفضاء الرقمي

المطلب الثاني: مكونات وخصائص البنية الرقمية

المطلب الثالث:الفواعل وطبيعة علاقات القوى في الفضاء الرقمي

الفرع الأول:الفواعل الدولاتية

الفرع الثاني:على المستوى اللادولاتي

المبحث الثاني: مفهوم العسكرة الرقمية

المطلب الأول: تعريف العسكرة الرقمية وعلاقتها ببعض المصطلحات

الفرع الأول: تعريف العسكرة الرقمية

الفرع الثاني:علاقة العسكرة الرقمية ببعض المفاهيم القريبة منها

المطلب الثاني: جذور و نشأة العسكرة الرقمية

- في جورجيا و أكرانيا

- في المجر وبولندا

المبحث الثاني: العسكرة الرقمية الأمريكية

المطلب الأول: السياسة الرقمية الأمريكية

الفرع الأول:التحول في العقيدة العسكرية الأمريكية

الفرع الثاني:الإستراتيجية الدفاعية الرقمية الأمريكية الجديدة

المطلب الثاني :الاستراتيجية السيبرانية للولايات المتحدة الأمريكية

المطلب الثالث: تحديات الاستراتيجية الأمريكية

المطلب الرابع: عوامل نهوض القوة الرقمية الأمريكية

الفرع الأول:استراتيجية الشراكة التكنولوجية : فيروس ستوكسنت نموذجا

الفرع الثاني:الخصخصة التكنولوجية

1- تفعيل دور القطاع الخاص

2-تجارة الأمن الإلكتروني (من الاستثمار الالكتروني الى تجارة الأمن الالكتروني)

المبحث الثالث: الحرب الباردة الجديدة

المطلب الأول: التصعيد الروسي -الأمريكي: ردود الفعل الأمريكية في ظل الاختراقات الروسية

المطلب الثاني :نماذج التنافس الرقمي الروسي- الأمريكي

الفرع الأول: التدخل في الإنتخابات الأمريكية

الفرع الثاني: قضية كاسبرسكي

المطلب الثالث :معالم ميزان قوى جديد

خاتمة

المقدمة

مقدمة

رغم الثورة الكبيرة التي أحدثتها التطورات الفكرية والصناعية في وسائل القتال والصراع البشرية، والتي دخل بها العالم العهد النووي والكيميائي، إلا أن ابتكاره لوسائل الاتصال الالكترونية والتقنية والتي كان أهمها الحاسوب والانترنت كانت الطفرة التي حدثت في حقل العلاقات الدولية، فمع انهيار المنظومة الاشتراكية وسقوط جدار برلين ودخول مصطلح العولمة إلى المحافل الدولية، تحولت هذه الوسائل السلمية لأدوات يستخدمها البشر في نزاعاتهم، الأمر الذي أحدث تغييرا في نمط القوة المستخدمة، وبالتالي تحديث نمط العسكرة بالإنتقال من العسكرة التقليدية إلى العسكرة الرقمية تماشيا مع التهديدات الجديدة، حيث أفرزت ثورة المعلومات ثلاث عناصر هي :المعلومة و الفضاء الإلكتروني والطابع الإلكتروني، و نعتقد بتوطد علاقة وثيقة ما بين الفضاء الإلكتروني والأمن الدولي والتي نتجت من التوسع في تبنى الحكومات الإلكترونية، واتساع مستخدمي وسائل الاتصال في العالم .فظهر ارتباط التكنولوجيا بالتحولات في القوة، وبرز مفهوم القوة الإلكترونية الذي عرفه جوزيف ناي على أنه " القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني" ، ان هذه القوة الجديدة المرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها كما يرى ناي أصبحت حقيقة أساسية ومؤثرة نتيجة التطور التكنولوجي السريع الذي ساهم بفعل الثورة التكنلوجية و ثورة الاتصالات التي أفرزت لنا ما أصطلح على تسميته بالفضاء الرقمي الذي يعد مجالا جديدا للتفاعل في العلاقات الدولية ،بحدوث تحولات جديدة على مفهوم القوة

وبفعل العولمة التي اتخذت من هذا الفضاء الجديد آداتها الأولى تغيرت ملامح السياسات الدولية بشكل كبير

بعد أن أصبحت عسكرة الفضاء الرقمي واقعا ممارسا، وتحول بذلك أمن الفضاء الرقمي إلى مسألة أمن قومي ودولي،هذا الأخير الذي يعتبر أكبر وأوسع وحدة تحليل في العلاقات الدولية كونه مرتبط بأمن كل دولة في النسق الدولي كما يتطلب تحقيقه آليات عمل جماعية ، وفي ظل تحول الفضاء الرقمي لميدان تُمارس فيه كل أشكال العنف،ظهرت خطورته عن غيره من المساحات التقليدية في إطار قدرته على استيعاب عدد أكبر من الفواعل، حتى خارج إطار النظام السياسي، مع امكانية توفيره للقدر المطلوب من المعلومات التي تستلزمها نشاطاتهم غير السلمية،فضلا عن قيامه بتقليل المسافات وتخطى حواجز الدولة القومية والحواجز المادية والتقليدية فيما بينها،و هي المميزات التي جعلت جوزيف ناي يرى أن ما يوفره الفضاء الإلكتروني من مصادر قوة لمختلف الفاعلين على مختلف الأصعدة، يشكل تهديدا مباشرا للأمن الوطني و الدولي و، اذ أنه يوسع من دائرة التهديدات الأمنية التي تنتج عن الأفعال العنيفة التي قد تمارسها الفواعل المختلفة. وبحكم أن العديد من مميزات الفضاء السيبراني ساهمت في تشكيل أطر جديدة للعلاقات الدولية والممارسات السياسية الأمر الذي يفسر أهمية المصطلحات التي صيغت مؤخرا مثل السياسة السيبرانية ،النزاع الالكتروني ،الأمن الرقميو التي استخدمت كلها في الفضاء الرقمي لتوجد أنواعا جديدة من النزاعات والصراعات الدولية مع كل ما يصاحب أنشطة هذا العالم الرقمي من طرق دولية جديدة للتعاون أيضا.

فكثيرة هي التحولات التي ساهمت في ارتباط العالم المتزايد بالفضاء الالكتروني بعد أن غدا هذا الفضاء "قوة مؤسسية"في السياسة الدولية بمساهمته في تشكيل الفعل الاجتماعي في ظل المحددات الجديدة التي باتت تطبع الفعل السياسي، إلا أن تحول هذا الأخير نحو العسكرة برز جليا في مظاهر

بالغة الأثر أهمها الهجمات الرقمية وما تشكله من أخطار على أمن الفضاء الرقمي الذي غدا أمنا مشتركا بحكم ترابط المصالح الدولية وتشابكها في منصهر واحد.

ومع التطور الذي صاحب الأمر في مجالات سياسات الدفاع و الأمن، والذي شكل في ذات الوقت الدافع الذي جعل من أمن الفضاء الرقمي يحظى بأهمية متزايدة في أجندة الأمن الدولي في محاولة لمواجهة تنامي التهديدات ودورها في التأثير على الطابع السلمي لذات الفضاء.

فهل تنجح الجهود لمنع عسكرة المجال الرقمي أم تخضعه لضوابط محددة كما هو الشأن في العسكرة التقليدية أم أن جاذبية العسكرة الرقمية ستمهد لنمط جديد من أنماط سباق التسلح الذي تحول من عسكرة العتاد الى عسكرة الفضاء وصولا الى عسكرة العالم الافتراضي، كما أن الثورة التقنية والمعلوماتية في عالم المعلومات والمعرفة الالكترونية أفرزت بلا شك أنماطا جديدة للتهديدات يقف المجتمع الدولي بمجمل فواعله في خضم تفاعلاتها التي تمس بالسلم والأمن الدوليين والتي يواجه تحدياتها بالانخراط بلا تأخير يُحسب في موجة العسكرة الرقمية التي تجر الدول نحو تسلح غير مرئي يعمل بوتيرة سريعة وتهدد بنشوب حروب افتراضية لا نقف على مجرياتها وإنما يمكننا معاينة آثارها.

1- **التعريف بالموضوع:** من خلال هذا التقديم والذي يأخذ شكل المعطى النظري فإن عنوان البحث المعتمد في هذه الدراسة تم تحديده بـ"العسكرة الرقمية و تأثيرها على أمن الدول
دراسة حالة :التنافس الرقمي الروسي- الأمريكي"

2- **أهمية الدراسة :**

على المستوى العلمي :

- تكمن الأهمية النظرية للدراسة في تناولها أحد المواضيع والمجالات البحثية الجديدة في مجال العلاقات الدولية، وهي العسكرة الرقمية كأحد أهم المجالات التي تمارس فيها التفاعلات الدولية،
- كما تتجلى أهمية البحث في محاولة للوقوف عند أهم كبريات نظريات العلاقات الدولية ومدى قدرتها على اعطاء تفسير للتحول الذي شهدته العلاقات الدولية بفعل الثورة التكنولوجية والتقنية سواء في طبيعتها أو في مظاهرها، اذ نسجل تحول العلاقات الدولية إلى جملة من الشبكات، كما هو الحال على مستوى الفواعل وذلك بالتخلي عن الفاعل التقليدي –الدولة – لصالح فواعل أخرى من غير الدول نظرا لقدرتهم على امتلاك القوة الإلكترونية وتوظيفها.
- تأتي أهمية العسكرة الرقمية كقضية تترجم التفاعلات الدولية الراهنة و التي مهد ارتفاع وتيرة التقدم التكنولوجي التقني الالكتروني في تحويل الفضاء الرقمي الى حقل دراسي يعج بالقضايا الأمنية الساخنة و التي تتفاقم تداعياتها في ظل ازدياد الاعتماد الدولي عليه خاصة مع تصاعد وتيرة الهجمات الرقمية التي تستهدف البنية التحتية الكونية للمعلومات من طرف قراصنة الانترنت أفرادا كانوا أم جماعات ،دولا أم عصابات .

3- **أهداف الدراسة :** تهدف هذه الدراسة أساسا إلى معرفة آثار العسكرة الرقمية على العلاقات الدولية والسياسات العالمية لما لها من أهمية تصل حد ضلوعها في الإخلال بالسلم والأمن الدوليين. وتهدف هذه الدراسة البحثية إلى :
- النظر في الأبعاد الأمنية والسياسية الخطيرة التي ينطوي عليها التسلح الرقمي .
- فهم العلاقة بين أمن المعلومات و الأمن الوطني و الدولي.

- الاطلاع على الدور الذي تلعبه العسكرة الرقمية في طرح تهديات جديدة، مع إمكانية حدوث حرب باردة جديدة بين الولايات المتحدة و روسيا.

4- **أسباب اختيار الموضوع**: يمكن تصنيفها إلى أسباب ذاتية وأخرى موضوعية وسيتم ذكرها على النحو التالي:

أ- الأسباب الذاتية:

- الرغبة في البحث و التقصي لاكتشاف المفاهيم الجديدة التي يطرحها ميدان العلاقات الدولية كالعسكرة الرقمية و الأمن الدولي الالكتروني .

-إن مجال التخصص الأكاديمي للطالبة في مجال الدراسات الأمنية ولد لديها رغبة للاهتمام بدراسة هذه الموضوعات المتعلقة بالعسكرة والأمن الإلكتروني.

- قلة الدراسات العربية في تناول موضوع العسكرة الرقمية بكل مفاهيمه وما ارتبط به كمجال بحثي وأكاديمي جديد ،ولد لدى الطالبة الاصرار على المساهمة بتدعيم الموضوع بهذه الدراسة المتواضعة.

ب- الأسباب الموضوعية: وردت كالأتي:

- إن أغلب الدراسات التي تناولت الموضوع كان بعنوان القوة الإلكترونية، كما كانت ضمن مواضيع مستقلة كالردع الإلكتروني والصراع الإلكتروني، لذا فالبحث يعمل على الربط بين العسكرة الرقمية كإختلاف عن القوة الإلكترونية وعلاقتها بالأمن الدولي.

- إن الأخذ بدراسة التنافس الإلكتروني بين روسيا والولايات المتحدة الأمريكية كطرفي صراع تنافس تقليديين مع محاولة معرفة استمرار صراعهما وتنافسها في المجال الرقمي-الإفتراضي

5- **إشكالية الدراسة**: انطلاقا من مسلمة أن هدف البحث العلمي الأساسي هو الوصول إلى الحقيقة وأن البحث يسير نحو بناء تراكمية معرفية في مجال العلاقات الدولية، تسعى هذه الدراسة للحصول على إجابة **للإشكالية التالية**:

"ما هي تداعيات العسكرة الرقمية على الاستقرار والأمن الدوليين وماهي الإستراتيجيات التي تضعها الدول لمواجهة تهديدات الفضاء الرقمي؟"

الأسئلة الفرعية :تتفرع عن هذه الإشكالية عدة أسئلة فرعية هي:

- ماهو الفضاء الرقمي والعسكرة الرقمية؟ وما هو دور الفضاء الرقمي في إبراز نمط جديد من التهدايدت الأمنية وفي تصعيد مظهر جديد من مظاهر الصراع والحرب ؟

- هل العسكرة الرقمية بديل كلي عن العسكرة التقليدية كشكل مختلف تماما عنها أم أداة من أدواتها الحديثة؟

- ما هو دور المجتمع الدولي في مجابهة آثار عسكرة الفضاء الرقمي في ظل الجهود المبذولة للحد من التسلح؟

فرضيات الدراسة :

تتمثل فرضيات الدراسة الأساسية فيما يلي :

- "كلما زادت نسبة التطور التكنولوجي التقني كلما زادت معها نسبة التوتر في العلاقات الدولية".
- "كلما سعت الدول لتحديث منشآتها الحيوية كلما زادت معها هشاشتها ونسبة تعرضها للخطر وعدم قدرتها للسيطرة على التهديدات الجديدة".

6- تفصيل الدراسة :

تنقسم هذه الدراسة البحثية إلى ثلاثة فصول ،اثنان منها خصصا لمعالجة ظاهرة العسكرة الرقمية من جانبها النظري أما الفصل الثالث فخصص للجانب التطبيقي أي قدمت فيه دراسة حالة . ونبتدئ الفصل الأول بالتطرق لمفهوم الفضاء الرقمي بسبب كونه مفهوما جامعا أشمل من ظاهرة العسكرة الرقمية مع الإسهاب في تفصيل مكوناته وخصائصه بغية تحديد المجال الذي تدور في فلكه الظاهرة موضوع الدراسة وبغرض تبيان علاقة الفضاء الرقمي بإحداث التغيير في البيئة الأمنية الدولية، كدوره في تغيير موازين القوى الدولية،و طرحه لمتغيرات جديدة ساهمت في بلورة فكرة عسكرته كتعدد الفاعلية في خضمه و خصائص استخدام القوة الرقمية في إطاره، ثم تناولنا مفهوم العسكرة الرقمية تعريفها و نشأتها وعناصرها وأنماط استخدامها مع عرض لآلياتهاو أشكالها و صورها، واختتمنا الفصل الأول بمحاولة لتحديد أطر العسكرة الرقمية النظرية و ذلك بمحاولة ايجاد نماذج تحليلية لها في كل من نظريات العلاقات الدولية التفسيرية و التحليلية بهدف وضع تأطير أصيل للظاهرة موضوع الدراسة.

أما الفصل الثاني فقد حاولنا فيه مناقشة قضية تأثير العسكرة الرقمية على الأمن الدولي من جوانبها المتعددة و لم يتأتى ذلك دون التفصيل في قضايا الأمن السيبيراني و التي مثلت تحولا في تهديدات الأمن القومي و الدولي وسياسات و طرق المواجهة الدولية لها.

وقد حاولنا في الفصل الثالث استعراض ومناقشة كل من العسكرتين الرقميتين الروسية و الامريكية في ظل التنافس المحتدم بينهما اذ بحثنا في هذا الفصل عن سر التفوق الروسي و فعالية الاستراتيجيات الرقمية الروسية كما عالج ذات الفصل تطور العسكرة الرقمية الأمريكية وتحدياتها المختلفة كما لم نغفل ايلاء التصعيد الروسي- الأمريكي و سباق التسلح الضاري حقه من البحث والتحليل.

7- المقاربات المنهجية:

بغية الوصول إلى إجابات وافية عن التساؤلات المطروحة في الدراسة المقدمة، وفي محاولة للتحقق من صحة الفرضيات المقدمة ومن منطلق أن الدراسة كانت وصفية تحليلية تم اعتماد المناهج التالية:

- **المنهج النوعي أو الكيفي**: والذي يتميز بإستكشاف الروابط الاجتماعية والتفاعلات وهو ما يناسب هذه الدراسة من خلال تفكيك العلاقة بين العسكرة الرقمية وتحديد تأثيراتها على الأمن الدولي، من خلال إبراز مفهومها وتحديد خصائصها وألياتها ومجالها السيبراني.
- **منهج دراسة حالة**: تم اللجوء إليه في الجانب التطبيقي للبحث في طبيعة التنافس والصراع السيبراني بين الولايات المتحدة الأمريكية وروسيا.
- **مقترب المجتمع العالمي:** هذا الاقتراب يتجه نحو التخلي عن التعريف القانوني في تحديد وحدات وفواعل العلاقات الدولية خارج الدولة ، فيُعرف تلك الوحدات وفقاً للصفة السلوكية، وهو ما يقصد به ان الفاعل هو كل من له القدرة على التأثير في مجرى العلاقات الدولية،
- **مقترب الحكم العالمي**، والذي يعمل على ابراز الفواعل غير دولتية، لدرجة تتطلب التحول من مفهوم الحكومة إلى مفهوم الحكم، كنتيجة لانتشار القوة في النظام الدولي. ويتم التركيز في هذا الإطار على مقترب الحكم العالمي، فيما يتعلق بتزايد دور الفاعلين من غير الدول وانغماسهم في السياسة العالمية، في الوقت الذي لا ينكر فيه دور الدولة، وإن كان متراجعاً .فالحكم العالمي وفقاً لهذا الاقتراب، هو نتاج للشبكة غير الهيراركية من المنظمات الدولية الحكومية، والمنظمات غير الحكومية، بالإضافة للأنظمة عبر القومية، والتي تنظم سلوك الفاعلين في القضايا عبر الوطنية.

8- **حدود الدراسة :**(مجال الدراسة)

- **حدود الدراسة الموضوعية :**تدخل هذه الدراسة ضمن أبحاث الأمن والدراسات الأمنية، بدراسة الفضاء السيبيراني مكمجال أمني جديد، أي ضمن دراسات الأمن غير التقليدي كما يمكن إدراجها في الأبحاث المتعلقة بالأمن الدولي والسياسات العسكرية للدول خاصة منها تلك التي تعنى بدراسة التنافس المستمر بين الطرفين التقليديين الولايات المتحدة و روسيا.
- **حدود الدراسة المكانية** :بما أن ظاهرة العسكرة الرقمية ظاهرة دولية فمجال الدراسة يتسع ليشمل العالم أجمع نظرا لارتباطها بالشبكة العنكبوتية كما تركز البحث في النصف الشمالي من الكرة الأرضية خاصة منطقتي أسيا وأوروبا وأمريكا الشمالية أين حاولنا استقصاء تطبيقات العسكرة الرقمية في روسيا والولايات المتحدة الأمريكية.

الدراسات السابقة: بالنظر إلى الأدبيات السابقة بشأن الموضوع محل البحث نذكر منها على سبيل الذكر:

- دراسة إيهاب خليفة تحت عنوان :القوة الإلكترونية وأبعاد التحول في خصائص القوة، يرى الباحث أنه بفضل ثورة المعلومات والإنترنت بمواقعه المختلفة ظهر مفهوم الفضاء الإلكتروني، وأصبح أحد العناصر المؤثرة في النظام الدولي نتيجة أدواته الإلكترونية والقادرة على الحشد والتعبئة، بجانب التأثير على القيم السياسية، نتيجة قلة تكلفتها، وأنها لم تعد حكرا على الدولة فقط، وأصبح من يمتلكها لديه القدرة على التأثير على الفاعلين المستخدمين لهذه البيئة.

- دراسة لجوزيف ناي تحت عنوان cyber power : يرى جوزيف ناي أن القوة تعتمد على السياق، بينما السياق الجديد المؤثر في السياسة الدولية الآن هو النمو السريع للفضاء الإلكتروني، ومع انخفاض تكلفة الاستخدام وصعوبة الكشف عن الهوية أصبحت الجهات الفاعلة الصغيرة قادرة على ممارسة القوة الصلبة والناعمة عبر الفضاء الإلكتروني، وإن كان هذا الانتشار يقلل الفوارق في القوة بين الدولة والفاعلين من غير الدولة إلا أنه لا يعنى المساواة في القوة أو استبدال الحكومات والجهات الفاعلة الأكثر نفوذا في السياسة العالمية
- دراسة لعادل عبد الصادق :القوة الإلكترونية :أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني وفيها يستعرض الباحث المفاهيم المختلفة للفضاء الإلكتروني
- دراسة لسعاد محمود تحت عنوان" :ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية ترى الباحثة أن مفهوم القوة قد طرأت عليه مجموعة من المتغيرات لمواكبة التطور الحادث في السياسة الدولية، وأن مضمون وعناصر القوة يرتبطان بشكل أساسي بطبيعة المصادر الفعلية والمحتملة لتهديد الأمن، والتي ظهرت فعليا منذ الحرب الباردة والتي صاحبها مصادر جديدة لتهديد الأمن مثل التهديدات العابرة للحدود مثل :المخدرات والإرهاب.
- دراسة ل James A. Lewis تحت عنوان الإنترنت والإرهاب The Internet and Terrorism : يرى الباحث أن الشبكات الإلكترونية تسمح للجهاديين بالحفاظ على وجودهم والتنسيق فيما بينهم حول العمليات التي ستنفذها .وشبكة الإنترنت هي واحدة من هذه الشبكات .وهو مورد حيوي للإرهاب العالمي. ويعتقد الباحث أن الجماعات الإسلامية ليست الأولى في المنظمات الإرهابية في اللجوء للإنترنت، ولكنها تعلمت بسرعة قيمة التكنولوجيا الجديدة .وأصبحت باكستان مركزا أساسيا لمحترفي الإنترنت خاصة من جماعات عسكر طيبة الأصوليين.

الفصل الأول: تحديد المجال،ضبط مفاهيمي و تأصيل نظري للدراسة

ينبغي الاعتراف ان محاولة الضبط المفاهيمي للعسكرة الرقمية و التأصيل النظري لها مهمة تشوبها الكثير من الصعوبات المتعلقة أولا بحداثة المجال و ندرة المحاولات البحثية الخاصة بالموضوع بحد ذاته وثانيا التباين الواضح ازاء تناول موضوع الدراسة و الذي شكل في الوقت نفسه الاختلاف الذي حول من جوانب الظاهرة الى مواد شكلت مفاهيمها المتعددة نواة جديدة اعتمد عليها الباحثون بهدف صياغة تعريفات ملمة بموضوع العسكرة الرقمية و مجالها المتمثل في الفضاء السيبراني.

المبحث الأول:تحديد المجال:الانتقال من الجغرافيا للفضاء الرقمي.

شكل ظهور الفضاء الرقمي كمجال جديد في العلاقات الدولية تحولا كبيرا في حركة التفاعلات والتحولات **البنيوية** بعدما برزت حالة توظيفه في الاستخدامات المدنية والاخرى ذات الطبيعة العسكرية، وأضحى مثل غيره من المجالات الدولية كالبر والبحر والجو، وبدأ ينتقل تأثيره من احداث تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي ،وأصبح يشهد العالم تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي والانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف ، وأصبحت قضية أمن الفضاء االرقمي تلقى اهتماما متصاعدا على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الرقمي ،وباتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية – ذات الطبيعة الإلكترونية – إلى أخطار إلكترونية ،بعدما تحول الفضاء الرقمي لوسيط ومصدر لأدوات جديدة

للصراع الدولي المتعدد الأطراف[1]مما فرض تحديات تعلقت أساسا في دوره الكبير في تغذية التوترات وتعقيد النزاعات واطالة الصراعات وهو ما يستوجب النظر في المميزات و الخصائص الاستراتيجية التي يطرحها هذا الفضاء الواسع و التي تسمح عسكرتها بتهديد السلم و الأمن الدوليين.

المطلب الأول: تعريف الفضاء الرقمي

تعد ثورة المعلومات والإتصالات والإعلام المتعدد الوسائط هي أحد أبرز عمليات التحول التاريخي في المعرفة والقوة والثروة في تاريخنا المعاصر، فقد برزت تجلياتها على كافة المجالات الحياتية السياسية والأمنية والاقتصادية والإجتماعية والثقافية. ويعد ظهور الفضاء الإلكتروني أحد أهم ملامح تلك الثورة التي ساهمت في إفراز عناصر أساسية هي :الطابع الرقمي**"Digital"** والفضاء الرقمي "Digital space" أو ما يرادفها **"Cyber space"** وتعد كلمة Cyber مقتبسة من علم "Cybernetic" و التي تمثل" نظرية الإتصالات و التحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الإتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان ".[2] أي أنها تعني "علم دراسة الإتصالات والتحكم الآلي للنظم العصبية للكائنات الحية ومحاكاة الآلات منها" وهو علم قائم بذاته منذ سنة 1948 من قبل عالم الرياضيات الأمريكي نوربرت وينر[3]لا يجري تعريفه على الآلة فقط بل ينطبق على الحيوان أيضا، فهو يمثل علم علم النظم ،يعرف نفسه كمجموعة من عناصر التفاعل تتكون من تبادل المادة والطاقة و المعلومات و ردود الفعل و التنظيم الذاتي و التي تكون في مجملها علم التحكم الآلي.

و ترتبط كلمة **rCybe** بكلمة **space** لتعطي معنى الفضاء السيبراني أو الرقمي أو الإلكتروني الذي يمثل "كل الإتصالات والشبكات وقواعد المعلومات والبيانات و مصادر المعلومات"[4].

فالفضاء الرقمي أولا وقبل كل شيء بيئة للمعلومات من حيث تكونه من بيانات رقمية تم انشاؤها و تخزينها ومن ثم مشاركتها، إلا أنه ليس افتراضيا بحتا فهو يشمل الحواسيب و شبكة الانترنت، ورغم استعمالنا كلمة انترنت كإختصار للعالم الرقمي فالفضاء الرقمي يشمل أيضا

---

[1] - عادل عبد الصادق ،"القوة الالكترونية : أسلحة الانتشار الشامل في عصر الفضاء الالكتروني "، مؤتمر حروب الفضاء السيبيراني (2012) اطلع عليه بتاريخ 06 فيفري 2018
http://www.accronline.com/article_detail.aspx?id=4747

1 -ايهاب خليفة ،" القوة الالكترونية و أبعادالتحول في خصائص القوة"، (2014)، 17، اطلع عليه بتاريخ 08 فيفري2018 :https://www.bibalex.org/Attachments/PublicationslFile/2014070311292451794-awark12pdf.pdf

4- الفتلاوي ،أحمد عبيس ."الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"،(العراق :جامعة بابل ،2015)،614-615

الأشخاص خلف هذه الحواسيب[1] ، وهو بذلك مجال مركب مادي وغير مادي يمثل مجموعة من العناصر هي: "أجهزة الكمبيوتر، أنظمة الشبكات، البرمجيات، حوسبة المعلومات، نقل وتخزين البيانات ومستخدمو كل هذه العناصر"، غير أن هذه التعريفات لم توفي المفهوم حقه من الضبط بسبب التطور السريع الذي يتميز به الفضاء السيبراني، حتى أن وزارة الدفاع الأمريكي و التي تعد الأب الروحي للفضاء الرقمي واجهت صعوبات جمة في إعطاء تعريف محدد له نظرا للسرعة المتزايدة للتطور الذي يسير به و اتساع ما أنتجته . إن الفضاء الرقمي اليومي بالكاد نستطيع تميزه عن ما كان عليه في بداياته المتواضعة، فالفضاء الرقمي "ليس بناقل" بل مجموعة من "القنوات ""حسب تعريف تد ستيفنس عضو مجلس الشيوخ السابق في الأسكا، و كلمة قنوات مستوحاة من كلمة" أنابيب" و التي تستخدم من قبل المختصين في المجال لوصف اتصال البيانات و تقترب العلاقة بين العالم المادي والعالم الأفتراضي بكون الفضاء الرقمي يمثل المحتوى أو البديل الكوني "الذي يمكن الناس من المشاركة فيه". و حسب وصف وليام جيبسون فإنه يعني "العالم الرقمي" أي مجموعة "شبكات الكمبيوتر والإتصالات بما يكون فضاء الكترونيا"[2].

كما عرفه جوزيف ناي بأنه " نطاق تشغيلي محكم باستخدام الالكترونيات لاكتشاف المعلومات عبر أنظمة مترابطة ببعضها البعض و بنية تحتية لها "

وعرفه فريق جامعة الدفاع الوطني الأمريكية بأنه " مجال تشغيلي تجري فيه مجموعة من العمليات ذات الطابع الالكتروني ، ويتميز بأنه ذو طابع فريد و متفرد ،محكوم بمجموعة من الاستخدامات التي تعتمد على الالكترونيات و الأطياف الكهرومغناطيسية لانشاء وتخزين و ابدال و استغلال المعلومات من خلال مجموعة من نظم المعلومات المترابطة والمتصلة عبر الانترنت و البنى التحتية الخاصة به"

خلاصة فالفضاء الالكتروني يمثل مكونا كهرومغناطيسيا تتفاعل فيه عناصر مادية و بشرية و معرفية بما يشكل مجالا حياتيا افتراضيا منتجا.

ببساطة فإن كل المجالات الحياتية من التجارة والصناعة والخدمات وصولا للاتصالات بما يكون البنية التحتية الحيوية للدول أضحت تُدار كلها بما كون شبكة عالمية من الشبكات.هذه البيئة الرقمية الجديدة التي شكلت عالما افتراضيا موازيا نقل له العالم الواقعي تفاعلاته وصراعاته. فإلى جانب الإستخدامات السلمية له ظهرت استخدامات غير سلمية عبرت عن التزاوج بين تكنولوجيا الإتصالات و المعلومات و الحرب مما خلق أحد أعقد القضايا الدولية ليس فيما تطرحه من إشكاليات فحسب بل في التكتيكات و الاستراتيجيات المصاحبة للعمليات غير السلمية الجارية على صعيده و كذا طبيعة التحديات التي يطرحها أين ظهرت العلاقة ما بين الفضاء الإلكتروني والأمن الدولي فمع التوسع في تبني الحكومات الالكترونية من جانب عدد كبير من الدول و اتساع

1- صباح عبد الصبور عبد الحي ،"استخدام القوة الالكترونية في التفاعلات الدولية- الجزء الثاني"، المعهد المصري للدراسات،(2015) ، اطلع عليه بتاريخ04 فيفري 2018

https://eipss.-eg .org /استخدام –القوة – الالكترونية – في – التفاعلات – الدولية – الجزء – الثاني/

[2] - بيتر وارن سينغر و ألن فريدمان، الأمن الالكتروني و الحرب الالكترونية ، تر مجاهد فخر الدين قاسم احمد (السودان: بحث تكميلي لنيل درجة الماجستير في الترجمة ، جامعة السودان للعلوم و التكنلوجيا)،16 و17و18، أطلع عليه بتاريخ 02 مارس 2018
Repository.sustech.edu/bitstrem/handle/123456789 /14861/66-281%20%الصفحات20%ترجمة
.pdf?sequence=1&isAllowed=y

نطاق مستخدمي وسائل الاتصال و تكنولوجيا المعلومات عبر المعمورة بشكل أصبحت المصالح القومية التي ترتبط بالبنية أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة للخطر بسبب تزايد اعتماد الدول على أنظمة التخزين "DATA "هو ما جعل قواعد البيانات القومية في حالة انكشاف خارجي بعد أن غدت منشآت حيوية كالطاقة و الإتصالات و المواصلات والخدمات الحكومية المختلفة و المؤسسات المالية و المصارف و التجارة الالكترونية كلها مرتبطة ببعضها البعض في بيئة عمل واحدة تعرف بالبنية التحتية القومية للمعلومات، ومرتبطة في الوقت نفسه بالبنية التحتية الكونية للمعلومات والتي تكونت بفعل الاعتماد المتزايد للدول على الأنظمة الالكترونية مما حولها لأهداف سهلة بما أنها تحمل طابعا مدنيا و عسكريا مزدوجا ،فقد وجدت تكنولوجيا الاتصال نوعا جديدا من الضرر الذي يمس بالمصالح القومية بسبب قابلية التعرض للهجوم دونما الحاجة للدخول الطبيعي والمادي لإقليم الدول[1]، إضافة للعولمة التي اتخذت من طرف الأنترنت آداة لتحويل العالم المادي إلى عالم افتراضي أين تعكس علاقات البشر التنافسية الصراعية و التعاونية ، لقد ساهم الطابع التكنولوجي في إيجاد طرق جديدة للصراع بديلة عن الحرب المباشرة بين الدول[2] بعد أن ساعدت الآليات التكنولوجية الفضاء الرقمي الدول و المنظمات و الأفراد للتفاعل فيما بينهم بعيدا عن الاتصال المباشر.

ان صعوبة فرض الرقابة التقليدية على التفاعلات الالكترونية جعلت من الفضاء السيبراني بيئة جذابة لممارسة الصراعات المعلوماتية خاصة بعدما ثبت إسهامه في دعم قدرة الأجهزة الأمنية للدول و حتى الجماعات المختلفة و هو ما دفع لتوظيفه بغية تحقيق أهداف سياسية و عسكرية مختلفة، الأمر الذي لم يرفع من درجة المخاطر فحسب بل وسع من ساحة الصراعات و نوع وسائلها و أهدافها وغدا بذلك الانترنت أحد معالم المجتمع الحديث و أكثرها تأثيرا و تأثرا وبحكم كون الفضاء الرقمي "محيط لا متناهي"فانه تحول لمكان خطر يهيمن عليه قانون الأقوى، مما يطرح عدة تحديات لرجال السياسة و الأمن.اذ تصاعد دوره في حركة التفاعلات والتحولات البنيوية على الساحة الدولية ونقل تأثيره من احداث تغيرات هيكلية إلى إحداث تغيرات كيفية في النظام الدولي،و اقترن التطور في مراحل النضج التكنولوجي بالتطور في حجم و نوع المخاطر الأمنية الوطنية و الدولية،و تحولت بذلك مفاهيم و تطبيقات الأمن و القوة و الصراع و الأزمة في العلاقات الدولية لتأخذ معاني و مفاهيم جديدة و مختلفة و قد تجلى ذلك في توظيف الفواعل المختلفة للفضاء السيبراني في الاستخدامات العسكرية له عبر نمطين، تعلق الأول باستعمال القوة الناعمة في الصراع و ذلك عن طريق توظيف حرب الأفكار و العمليات النفسية بعدما برز دوره في تصاعد الأفكار و تشكيل الصور المرئية والذهنية والرموز الثقافية في العلاقات الدولية كما عبر النمط الآخر عن استعمال القوة الصلبة و ذلك باستعمال شتى الأسلحة الالكترونية في إدارة وتنشيط العمليات العدائية[3] . وبهذا فقد خلق دخول شبكات الإتصالات والمعلومات بيئة ومجال

---

[1] -عادل عبد الصادق ،"الارهاب الالكتروني و القوة في العلاقات الدولية نمط جديد وتحديات مختلفة"، مركز الدراسات السياسية و الاستراتيجية (2009) اطلع عليه بتاريخ 27 فيفري 2018
http://accronline.com/book_detail.aspx?id=75

[2]-نبيل عبد الفتاح ، "مقدمة للارهاب الالكتروني والقوة في العلاقات الدولية نمط جديد وتحديات مختلفة"، مركز الدراسات السياسية والاستراتيجية،2009)أطلع عليه بتاريخ 25 فيفري2018

http://accronline.com/book_detail.aspx?id=75

2-عادل عبدالصادق ،"عسكرة الفضاء الالكتروني،بين التحديات و فرص المواجهة"،مجلة لغة العصر ،مؤسسة الأهرام،عدد مارس(2017) اطلع عليه بتاريخ 06 مارس2018

الاستخدامات الحربية الاعلان عن نوع جديد من العسكرة ألا و هو العسكرة الرقمية أو عسكرة الفضاء الرقمي.

المطلب الثاني: مكونات وخصائص البنية الرقمية.

كأي فضاء يتركب الفضاء السيبراني من مجموعة من العناصر الأساسية والتي تشكل البنية الرئيسية للفضاء الرقمي مع تميزه في ذات الحين بجملة من الخصائص التي تطبع المجال الرقمي و تشكل الاختلاف الذي يطغى على كل النشاطات الدائرة في فلك البيئة السيبرانية .

أولا: مكونات الفضاء الرقمي:

خلافا للفضاء التقليدي تشكل العناصر الأساسية الثلاث المتكونة أساسا من العنصر المعرفي و العنصر البشري والعنصر المادي البنية التحتية الرئيسية للفضاءالسيبراني و المتمثلة في:

أ- الأنترنت: تعد العصب المحرك للفضاء الرقمي فهو يلعب الدور الأبرز في الثورة المعلوماتية والتكنولوجية التي يشهدها العالم منذ بداية القرن الواحد والعشرين فقد تم إرسال اول بريد الكتروني سنة 1971 اليوم يرسل ما يقارب الأربعين ترليون بريد الكتروني في السنة . و قد تم افتتاح أول موقع على الأنترنت عام 1991 و بلغ عدد الصفحات على الأنترنت ما يزيد عن 30ترليون صفحة بحلول عام 2013. لم يعد الأنترنت يقتصر على إرسال بريد الكتروني او جمع معلومات بل أصبح يتعامل مع كل شيء و قد قدرت سيكو التي تعتبر احدى الشركات التي تساهم في تشغيل العمود الفقري الأنترنت أنه بنهاية عام 2012 وصل عدد الأجهزة الموصولة بالأنترنت 8.17 بليون جهاز و تقدر الاحصائيات أنه بحلول عام 2020 سيصل عددها إلى 40 بليونا[1].

ب- المعلومة: تعد المعارف والمعلومات المورد الرئيسي في الحياة[2] الأقتصادية والسياسية فضلا عن الأثر الذي تحدثه في حسم الصراعات الدولية و يتميز الفضاء الرقمي بتدفق هائل من حيث الكم والكيف المعلوماتي.

ج- الحاسوب: هو الأداة التي تتم بواسطتها عملية الإتصالات ومن ثم المشاركة في عملية صنع القرار الدولي .

وبهذا فالفضاء الرقمي يشكل بنية متكاملة تتكون من ثلاث طبقات:

(http://www.accronline.com/article_detail.aspx?id=28402[3]

1-جوزيف تاي،"القووة الناعمة وسيلة النجاح في السياسة الدولية "،تر د. محمد توفيق البجيرمي (السعودية:العبيكان ،الطبعة العربية الأولى، 2007)ص اطلع عليه بتاريخ12فيفري2018
https://www.scribd.com/document/366354634/القوة-الناعمة-جوزيف-ناي-pdf

[2]- اسماعيل قادير ،"ادارة الحرب النفسية في الفضاء الالكتروني :الاستراتيجية الامريكية الجديدة في الشرق الاوسط" (ورقة مقدمة للندوة الدولية حول عولمة الاعلام- السياسي و تحديات الأمن القومي للدول النامية ،كلية العلوم السياسية و العلاقات الدولية ،جامعة الجزائر 3)Ismail_enssp@yahoo.com

- الطبقة المادية: والتي تشمل الحواسيب والبرمجيات والمعدات الخاصة بالربط البيني.

- الطبقة المنطقية: وتتخذ بعدا تقنيا إذ تشمل مجموعة البرامج التي تحول المعلومات إلى معطيات رقمية أي يتم خلالها الإنتقال من لغة التناول إلى لغة البرمجة.

- الطبقة الإعلامية: و تستخدم البعد الإجتماعي عنوانا لها حيث تشمل الهويات الرقمية (العنوان والبريد الإلكتروني للمستخدم و رقم هاتفه النقال فضلا عن الصور الرمزية له على مواقع التواصل الإجتماعي[1].

إن هذا العالم الموازي شأنه شأن الفضاء التقليدي تحدده مكونات رئيسية هي **المكان والمسافة والحجم والمسار**، غير أنه يتميز بغياب الحدود الجغرافية، وهو ما أضفى عليه صفة الخطورة كونه لا يمكن التحكم والسيطرة على مدخلا ته ومخرجاته.

ثانيا: خصائص الفضاء الرقمي

من حيث كونه بيئة افتراضية أساسا فالفضاء الرقمي عالم تطبعه الكثير من الميزات الجديدة التي تجعله فريدا من نوعه تتداخل فيه العوامل الذاتية والموضوعية لتنصهر كلها في بوتقة عالمية تتداخل فيها المصالح الشخصية وتسمح في الوقت نفسه ببلورة الأهداف الجماعية بشكل سريع ودقيق في آن واحد.

- **العالمية**: و هي أمر لا يقتصر على الأنترنت فحسب بل هي عالمية تحكمها ترابط الشبكات الإجتماعية اللاسلكية للهاتف وغيره[2].

- **الجدة** :كون الفضاء الرقمي بشري المنشأ[3] والإستخدام، فإنه بدا واضحا إدراج البعد الإجتماعي فيه بعد أن غدا الفرد فاعلا استراتيجيا مما طرح إشكاليات إمكانية التحكم أو حتى توقع سلوكات هذا الأخير الذي ما يفتأ يظفي على المجال الرقمي صفة التجدد والتطور المصاحبة للسلوك البشري و التي تعزى للنشاطات المستمرة الدائرة في فلك الفضاء السيبيراني.

- **مجهولية تحديد المصدر**:وهي الخاصية التي تقابلها خاصية أخرى شكلتا الاثنتان سمتان مميزتان للفضاء الرقمي، فرغم تمييز العالم السيبراني إن جاز القول بالشفافية المطلقة وسهولة الوصول لجميع البيانات "attribution"، فهو في نفس الوقت يمثل مساحة مبهمة تمكن للمتخصصين بالمجال من تنفيذ عدة إجراءات مخفية يكون لهم علم واسع بتقنياتها وطرق الولوج إليها، و هو ما خلق خاصية خطيرة تميز بها هذا الفضاء وهي عدم إمكانية تتبع الفاعلين فيه بما يعد

---

[1] -قادير ،"ادارة الحرب النفسية"،مرجع سابق

[2] - Richard A. Clarke and Robert K. Knake , « cyber war »,Harper Collins e- Books, 38 http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20

[3] - ربيع محمد يحي،اسرائيل و خطوات الهيمنة على ساحة الفضاء السيبيراني في الشرق الأوسط :دراسة حول استعدادات و محاور عمل الدولة العبرية في عصر الأنترنت "2012 2013"(مصر :الهيئة العامة المصرية للكتاب،2010)67 أطلع عليه بتاريخ 25فيفري2018 http://strategicvisions.ecssr.com/ECSSR/ECSSR_DOCDATA_PRO_EN/Resources/PDF/Rua_Strategia/Rua-Issue-03/rua03_064.pdf

أمرا جديدا تماما من الناحية الإستراتيجية فالواقع أن الفضاء السيبراني ليس مبهما فحسب بل يقدم للفاعلين الذين يستخدمونه قواعد إستراتيجية جديدة للتحرك من خلاله.

- **السيولة**:والتي تواكب خاصية الجدة بما أن الفضاء الرقمي يُظهر تغيرات مستدامة وإعادة تكوين متواصلة وموازاة مع المميزات التي شكلت من الفضاء الرقمي ساحة تفاعلات فريدة من نوعها فإنه يفتقر للقوانين الوضعية اللازمة والتي تستهدف ضبط سياسات الفواعل تجاه بعضها البعض بسبب

تجاوزه آليات المسؤولية بحكم تجاوزه قيود الجغرافيا [1]والموقع المادي وخاصية التخلل التي تعني اختراقه لحدود الإختصاصات القضائية.

المطلب الثالث:الفواعل وطبيعة علاقات القوى في الفضاء الرقمي

تتعدد الفواعل في الفضاء الرقمي و يتوزعون على مستويين:مستوى دولاتي ومستوى لادولاتي.
1- على المستوى الدولاتي: تعتبر الدولة الفاعل الأساسي وذلك راجع لمحورية دورها في الفضاء الرقمي وما يتطلبه الأمر من إمكانات مادية و بشرية قانونية وبنيوية . اذ تقوم الدول برصد ميزانيات كبيرة و تسخير جهود معتبرة مع اعداد استراتيجيات محكمة في محاولة منها للتحكم في التفاعلات التي تجري على صعيد الفضاء السيبراني .

2- على المستوى اللادولاتي:تزاحم الدولة فواعل تظهر أهميتهم في حجم التهديد الذي يحدثونه يمكن تقسيمها الى مستويين : فواعل ما دون الدولة و فواعل ما فوق الدولة.

أـفواعل ما فوق الدولة : أصبحت حقيقة و جزء لا يتجزأ من واقع العلاقات الدولية بعد ان امتدت تأثيراتها إلى خارج حدود الدولة" **فقد أصبحت قريبة من المواطن أكثر من مؤسسات الدولة**، أو ما عبر عنه الكاتب و المختص في العلاقات الدولية "جوزيف ناي" في مؤلفه القوة الناعمة بالقدرة على اجتذاب الافراد و القوى الفاعلة :[2]

- المنظمات الدولية و الاقليمية:. بإثباتها معايير الفاعل الدولي تسعى المنظمات الدولية و الاقليمية لأن تحظى بلقب الفاعل العالمي الرسمي الذي تكون قراراته أسمى من أن تطالها سلطة الدول .
- المنظمات غير الحكومية: و التي تواجه معارضة شرسة من طرف الوحدات الدولية بسبب اعتمادها على الانترنت لتعبئة الرأي العام و الضغط على الحكومات من خلال تعبئة المجتمع المدني و تنظيم الحملات الاجتماعية و من ابرز أمثلتها منظمة البيئة العالمية و ما تقوم به من ضغوطات مختلفة على الحكومات.

2-عادل عبد الصادق "أنماط الحرب السيبيرانية وتداعياتها على الأمن العالمي"،مجلة السياسة الدولية ،عدد ماي(2017) أطلع عليه بتاريخ 26فيفري
2018
http://www.siyassa.org.eg/News/12072.aspx

[2] جوزيف س ناي ،القوة الناعمة وسيلة النجاح في السياسة الدولية،تر د. محمد توفيق البجيرمي (السعودية:العبيكان ،الطبعة العربية الأولى، 2007)ص اطلع عليه بتاريخ12فيفري2018
https://www.scribd.com/document/366354634/القوة-الناعمة-جوزيف-ناي-pdf

- **المنظمات الافتراضية** : .تم إنشاء منظمة خاصة بالمواطن العالمي بمبادرة من الأعضاء المؤسسين لمنظمة الإنسان العالمي في جمهورية أوكرانيا الاتحادية ليكون بيت لجميع المؤمنين بعالم واحد يضم تحت رايته بعدل و رحمة وحرية وليكون مكانا لجمع كل الأفكار الإنسانية لتصبح مرجعا ودستورا عاما. و اتخذت جمهورية أوكرانيا مقرا لها. و تعمل على تشكيل فروع لها في كافة دول العالم كطريقة أولى لبداية نشر فكرة المواطن العالمي أو الكوني. و هي من أوائل المنظمات غير الحكومية الافتراضية لإسماع الأصوات العالمية[1]. و من المتوقع أن انتشار استعمال الوسائط الالكترونية سيروج كثيرا لفكرة المواطن العالمي و الذي سيصبح فاعلا دوليا نشيطا سواء تكتل تحت لواء منظمة عالمية غير حكومية افتراضية أم غير افتراضية، ليضيف نوعا و نمطا جديدا للحياة السياسية العامة الدولية . إنه عصر السباق الرهيب بين الفواعل الجديدة لإثبات القدرات و الموارد ، القدرة على المواصلة،و الكفاءة والفعالية و بالتالي الحكامة الرشيدة لتفرض نفسها في عصر التنافسية هي القاعدة الأساسية التي قامت عليها الليبيرالية" Bas de formulaire"[2]

ب-فواعل ما دون الدولة : رغم ان التسارع المفرط في نشوء فواعل ما دون الدولة وتنامي نشاطاتها لم يقابله تسارع مماثل في تطوير الأطر النظرية التي تسمح باستيعابها بوصفها فواعل مؤثرة في العلاقات الدولية ورغم كون هذا النمط من الفاعلين أقل حظا بالاهتمام الأكاديمي اذا ما قورن بالاهتمام المخصص للفاعلين من غير الدول من فئة "فواعل ما فوق الدولة " فان التهافت الحاصل تجاه فرضية تراجع محورية القوة العسكرية في توجيه تفاعلات عالم ما بعد الحرب الباردة لفائدة الفواعل من غير الدول وينقسمون الى خمس فئات:

- المجرمون الفرادى : الهاكرز
- الجماعات الاجرامية: تستهدف الربح النقدي
- الجواسيس: يستهدفون سرقة معلومات سرية الخاصة بالحكومة او الجهات الامنية
- محاربي الدولة :الذين يطورون القدرات و ينفذون هجماتالكترونية دعما لأهداف استراتيجية للبلد
- الارهابيون :الذين ينخرطون في الهجمات الالكترونية [3]

- **1- الفرد**: بفعل تأثير الفضاء السيبيراني بات الفرد فاعلا يحسب له ألف حساب، فبفعل سهولة وصوله وتحكمه في الوسائل الالكترونية المتطورة ازداد الاهتمام به من كثرة تدخلاته المستمرة محاولة منه إصلاح أوضاع مجتمعه الصغير الدولة و أوضاع مجتمعه الأكبر العالم مما أتاح لفكرة المواطن العالمي le citoyen universel للظهور من جديد[4] بعدما أصبح العالم قرية صغيرة بفعل الثورة التكنولوجية و التقنية و المعلوماتية التي ساهمت في تطوير و ترقية مختلف وسائل الإعلام المسموعة منها المكتوبة المرئية قنوات فضائية يربط الانترنت اجزاءها المترامية الأطراف.

---

[1]- نبيلة بن يوسف ،"مستقبل العلاقات الدوليةفي ظل وجود فواعل جديدة ..المنظمات العالمية غير الحكومية "و "المواطن العالمي"،21، fr.yahoo@kadem.ballni أكتوبر2012
http://kenanaonline.com/users/nabilabenyoucef/posts/463015

[2] -بن يوسف ،"مستقبل العلاقات الدولية"، مرجع سابق

[3] -- شهرزاد ادمام ،" الفواعل العنيفة من غير الدول :دراسة في الأطر المفاهيمية و النظرية"،المنهل :مجلة سياسات عربية ،العدد الثامن مارس (2014)،21
أطلع عليه بتاريخ30 أفريل 2018
https://platform.almanhal.com/Files/2/50789

[4] --بن يوسف ،"مستقبل العلاقات الدولية"، مرجع سابق

وكما صرح مسؤول أمريكي قبل سبعة عشر عاما أن الانترنت سيحقق للعالم ما عجز عن تحقيقه في مجال الديمقراطية ذلك لأنه "سيحقق الديمقراطية" فقد ساهمت الصحافة الالكترونية بالتركيز على القيم المشتركة بين شعوب العالم[1] وزيادة الوعي الجماعي وما يصاحبه من مخاطر اعادة توجيه الولاءات الوطنية، فضلا عن قدرته المتزايدة في استعمال القوة الصلبة وذلك بتصميم وانتاج شتى أنواع الفيروسات والديدان وتوجيهها نحو ضرب أهداف دولية استراتيجية بعدما تسنى للأفراد" hacker" حيازة القدرة على إحداث ثورة رقمية و من أبرز الأمثلة على ذلك :مارك زوكربارغ الذي استطاع عبر تأسيسه لشبكة فايس بوك استقطاب اكثر من مليار مستخدم [2]حول العالم. وقدازداد الاهتمام بالفرد من كثرة تدخلاته المستمرة محاولة منه إصلاح أوضاع مجتمعه الصغير الدولة و أوضاع مجتمعه الأكبر المتمثل في العالم.

2- **المجموعات الافتراضية**: او فاعلوا الشبكة ، وهم مجموعة بشرية (مادية حقيقية موجودة على أرض الواقع) تستخدم الوسط الافتراضي لإدارة مجموعة من الأفراد و توجههم باتجاه معين عبر التأثير المباشر أو غير المباشر من خلال تشكيل آراءهم بواسطة جملة من الأدوات الالكترونية و الوسائط المعنوية التي لها آثار مادية على أرض الواقع .و الفاعل في هذا المجال هو أي شخص يمتلك القدرة على أن يؤثر على مجموعة من الأفراد و يوجههم في الاتجاه الذي يريده عبر الوسط الالكتروني مثل (الفيس بوك و تويتر و انستغرام و غيرهما من مواقع التواصل الاجتماعي)، ومن أحدث تطبيقات هذا الفرع من فروع المعرفة الالكترونية ما قامت به مجموعة من الشباب العربي في تنظيم تظاهرات و إسقاط حكومات في المنطقة العربية (بغض النظر عن المسبب الرئيس والنتيجة النهائية) ، لكن كان لفواعل الشبكة أثر كبير في عملية التعبئة و الحشد والدعم والضخ الكبير للأفكار وإدارة الرأي العام و التفاعل عبر هذا الوسيط الالكتروني الجديد[3].

3-**المجموعات الارهابية** : برز دورها جليا بعد أحداث الحادي عشر من سبتمبر 2001 تحت صيغة الجماعات الارهابية ورغم أن الاهتمام كان منصبا في العلاقات الدولية أساسا على الموجة الأولى من الفواعل من غير الدول التي تنشط في المجالات السلمية من قبيل الشركات المتعددة الجنسيات والمنظمات القانونية الحقوقية والمهنية على حساب الموجة الثانية المتمثلة في تلك التي تنشط في المجال العسكري والتي تعد بعيدة نوعا ما عن سيطرة الدولة [4] ويتفاقم فيها دور القراصنة والذين تتنوع أهدافهم و غاياتهم، و من أمثلتها المجموعة الافتراضية المعروف "Anonymos" والتي تسوق لخطابات و مطالب سياسية مختلفة عبر أرجاء العالم.

لقد ساهم الفضاء السيبراني في زيادة الوعي بأهمية الابتكار والتقدم التكنولوجي كأساس للاستحواذ على القوة وأدى ذلك لتضاعف أهمية تطوير المفاهيم الاستراتيجية وتحقيق التقدم الاستخباراتي في المجال التقني و الاقتصادي ونظم الإتصالات بسبب تحول العنصر الرئيسي في بناء القوة من "الملكية إلى المعرفة و المعلومات " بمعنى أنه حدث تحول في مفهوم القوة على أساس الكم إلى القوة على أساس النتيجة المترتبة عنها، و هذا التحول قاد بدوره للتحول بمفهوم توازن القوى على أساس

---

[1] - بن يوسف ،"مستقبل العلاقات الدولية"،مرجع سابق.

[2] -قادير ،"ادارة الحرب النفسية"،مرجع سابق.

3-- كوثر الياسري،"الفواعل من غير الدول في العلاقات الدولية"،الحوار المتمدن ،العدد 4802 (2015)أطلع عليه بتاريخ 30ماي 2018 ،http://www.ahewar.org/debat/show.art.asp?aid=46737

1- أدمام ، ،"الفواعل العنيفة من غير الدول "،مرجع سابق.

"الثقل المعادل" من الدول إلى الفاعلين من غير الدول مما شكل تحديا لسيادة الدول، فظهور قضايا جديدة عابرة للقومية والتأثير الذي أحدثته ثورة المعلومات و الإتصالات عززت من خاصية انتشار القوة، هذه الخاصية الجديدة التي تقوم بتحدي نظام القطبية الذي يعتمد على توزيع هيراركي للقوة بين الدول ويدفع للاتجاه لنظام اللاقطبية ،فانتشار القوة لم يعد محصورا بين الفاعلين الأكثر قوة و ثروة فحسب بل يتسم باللامركزية أي ما بين مختلف الأفراد و الجماعات [1]إذ شكل الفضاء السيبراني بيئة مناسبة و جاذبة لمختلف الفواعل اللادولاتية التي تسعى لتحقيق أهداف سياسية و عسكرية و اقتصادية شتى.

كما ساهم الفضاء الالكتروني في تشكيل الفعل الإجتماعي و السياسي و العسكري مما حوله لقوة مؤسسية في السياسة الدولية ، و هو الأمر الذي أدى لتنامي حجم التهديدات التي تتربص بالأمن الدولي، فاتساع حركة الفاعلين قادنا للتساؤل عن الميزات الاستراتيجية التي بات يوفرها هذا العالم الافتراضي و التي أدت لتوظيفه في تعظيم قوة الدول من خلال إيجاد ميزة تأثير أوتفوق في البيئات المختلفة بعد أن أحدثت التطبيقات العسكرية السيبرانية ضررا في عملية توزيع الأدوار التي رتبت في السابق الدول في شكل هرمي من حيث الاعتماد على القوة العسكرية و التي سمح تحديد دورها و قدرتها على التدخل في المسرح الدولي[2]، و رغم أن القوى الكبرى لا تزال الأبرز حتى في هذا المجال بسبب امتلاكها لقدرات تكنولوجية هائلة و اعتمادها بشكل كبير على أنظمة المعلومات في إدارة شؤون الدولة ،[3] الا أن تصاعد دور الفرد ساهم بشكل كبير في التأثير على هيكل النظام الدولي و بنية علاقات القوى ، و إلى جانب دور الجماعات الارهابية برزت موجة ثالثة من الشركات المتعددة الجنسيات[4] و التي تركز على الخدمات و التطبيقات التكنولوجية و التي تفوق ميزانياتها ميزانيات دول بكاملها، و بهذا فقد أثر الفضاء الرقمي على طبيعة و أدوات و تحالفات السياسة الخارجية بل و غير من بنية الدبلوماسية الدولية مما زاد من أهمية دور التحالفات و الجهود الدولية و هو الأمر الذي أحدث فجوة تحليل نظرية كبيرة بين نظريات العلاقات الدولية البشرية في القرن العشرين و بين الحقائق الجديدة التي فرضتها عسكرة الفضاء الرقمي ، كما حدثت فجوة تحليل امبريقية بين المعلومات الموجودة و القياسات المطلوبة لتحليل اتجاهات الأنشطة عبر الفضاء السيبراني فضلا عن فجوات التحليل السياسية بين الممارسات التقليدية و الحاجة إلى أدوات تحليل جديدة . لقد ساهم الفضاء الالكتروني في دعم الهياكل التنظيمية و الاتصالية للحركات و الجماعات المحلية و المنظمات المدنية مما ساعد الفاعلين من غير الدول على ممارسة قوة التجنيد و الحشد و التعبئة و استجلاب الأموال[5].

ان انتقال جبهات القتال إلى ساحة الفضاء السيبراني كان له دور كبير في إعادة التفكير في حركية و ديناميكية الصراع و استعمال القوة البينية، مما خلف آثارا هائلة على مستوى طبيعة السياق الدولي

---

[1] - ناي،"القوة الناعمة"،مرجع سابق.

[2] -سعاد محمود أبو ليلة،" دور القوة :ديناميكيات التحول من الصلبة الى الناعمة الى الافتراضية"،السياسة الدولية (2012)،آخر تحديث 14 أفريل 2012 http://www.siyassa.org.eg/News/2376.aspx

[3] - "Cyberguerre :concept,état d'avencement et limites",Center for Security Studies(CSS),ETH Zurich,N 71,avril 2010 http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-71-FR.pdf

[4]- أدمام، "الفواعل العنيفة من غير الدول"،مرجع سابق

[5] - عادل عبد الصادق ،"أنماط الحرب السيبرانية"،مرجع سابق.

للفضاء الرقمي بتوفيره بيئة مناسبة ساهمت بدمج الفئات والقوى المهمشة في السياسة الدولية و خلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض.[1] فقد أدت عملية انتقال القوة من الدول بشكل عام إلى الفاعلين من غير الدول إلى صنع ظاهرة غير تقليدية فرضت تحديات شتى على الدول و هددت سيادتها. و قد عملت مميزات الفضاء الرقمي من حيث سهولة استخدامه و الرغبة المتزايدة في تبادل المعلومات على مضاعفة توزيع القوة بين عدد أكبر من الفاعلين على جعل هيمنة الدولة على هذا المجال صعبة التحقيق مقارنة بالمجالات الأخرى ، فقد سمحت القوة الالكترونية للفاعلين المجهريين في السياسة الدولية من ممارسة القوة الصلبة و الناعمة على حد سواء و قد مثل التهديد الأبرز في التساؤل الجديد لعنصر القوة الصلبة عبر الفضاء الالكتروني و الذي تمثل في التحول من اتخاذها كوسيلة " means " إلى اتخاذها كتأثير" effect" إلى زعزعة مفاهيم النفوذ و السلطة في النظام الدولي[2] .

المبحث الثاني: مفهوم العسكرة الرقمية

المطلب الأول: تعريف العسكرة الرقمية وعلاقتها ببعض المصطلحات

غزى تعبير العسكرة الرقمية الأوساط الأكاديمية منذ بداية القرن الواحد و العشرين كمرادف للاحرابية الرقمية والتي تعني **لغة:**

حسب المعجم للوسيط فلفظ العسكرة اسم و يعني لغويا الشدة و العسكر هو الجيش و مجتمعه و جمعه عساكر و العسكر هو الكثير من كل شيء و يقال وقعوا في عسكرة أي في شدة[3]. أما في المعجم الرائد فالعسكر هم الجنود و حسب معجم اللغة العربية المعاصر فنقول تعسكر الجيش في المكان أي تجمعوا[4] وهو ما يتفق معه المعجم الغني:عسكرة جند في ساحة:اي تجمعوا، أما لفظ الرقمية فهو اسم مؤنث منسوب إلى رقم و حسب معجم المعاني الجامع فالرقمية من رقم أي أنها مصدر رقم. و لغة الرقمية هي التي تعد خصيصا طبقا لقواعد معينة لتخدم للحاسبات الالكترونية كوسيلة للعمل به ومن ما سبق يمكننا القول أن العسكرة الرقمية هي جمع لمجالين الأمور العسكرية من جهة و لغة الأرقام من جهة أخرى.

اصطلاحا:يشير مفهوم العسكرة الرقمية "Digital Militarism إلى "كيفية استخدام تكنولوجيا الاتصال بما في ذلك آليات ووسائل التواصل الإجتماعي من اجل أغراض عسكرية سواء من قبل الدولة او بواسطة

---

[2] - نازلي شكري ،"السياسة السيبرانية في العلاقات الدولية "، تقدمة محمد مسعد العربي ،مجلة السياسة الدولية(2013)،آخر تحديث 20 نوفمبر 2013
http://www.siyassa.org.eg/News/3352.aspx

2-العسكرة،معجم الوسيط،قاموس المعاني ،أطلع عليه بتاريخ 03فيفري2018
https://www.almaany.com/ar/dict/ar-ar /العسكرة./
3-عسكرة ،معجم الرائد،قاموس المعاني، اطلع عليه بتاريخ03فيفري2018
https://www.almaany.com/ar/dict/ar-ar/?c=الرائد

4-العسكرة ،معجم الغني ،قاموس المعاني الالكتروني،أطلع عليه بتاريخ 03فيفري2018 .
https://www.almaany.com/ar/dict/ar-ar/

المستخدمين العاديين"[1] . و حسب المقاربة الأنثربولوجية "أنها عملية استحالت عبرها منصات التواصل الرقمي و الممارسات الاستهلاكية في العقدين الأولين من القرن الحادي والعشرين ، أدوات حربية في أيدي الفاعلين التابعين لأجهزة الدولة أو من غير العاملين فيها ، في حقلي العمليات العسكرية و الأطر المدنية" [2]، و عسكرة الفضاء الرقمي تعني استخدامه من طرف دولة ما في إعلأن الحروب و ما يستلزم ذلك من إصدار البيانات و نفي الاتهامات. كما يعبر عن الممارسات العنيفة التي تمم عبر الفضاء الرقمي كنشر الصور و المقاطع الحية من ميادين المعارك. و يشهد الفضاء الرقمي ازديادا مطردا لممارسات عنف الدولة عبره خلال السنوات الأخيرة خاصة الفترة التي شهدت أندلاع الثورات العربية اذ زاد معدل استخدامها وفي حين يمثل التعريف الثاني للعسكرة الرقمية رصد لآلية من آليات العسكرة الرقمية و المتمثلة في استخدام شبكات التواصل الإجتماعي وهو مايعبر عن التركيز على شكل من أشكال استعمال القوة الناعمة في إطار رقمي دون الاسهاب في ذكر استعمالات القوة الصلبة في ذات الاطار.

لطالما عبرت العسكرة عن إيديولوجية سياسة أو تيار فكري يدافع عن أولوية القوة العسكرية في العلاقات الدولية بين الدول والتنظيم داخل الدول، فقد عرفت العسكرة عددا لا يستهان به من نماذج التجسد عبر التاريخ، ادعى أنصارها أن الجيش هو أفضل آداة لخدمة الأمة و حماية مصالحها ،[3]و هو ما يدفعنا للتصريح بأن العسكرة الرقمية هي تجسيد آخر لهذه الأفضلية التي حولت من الفضاء الرقمي ميدانا آخر للقتال تدار فيه الحروب و تمارس فيه شتى أنواع العنف بغرض إفشال قوة الأعداء. عسكرة المعلومات أي تجنيد المعلومات لخدمة أغراض عسكرية و تحقيق أهداف عبر استغلال المميزات التي يوفرها الفضاء الرقمي و التي تسمح بتحقيق غايات و أهداف الدولة العليا. وقد شهدت التطبيقات العسكرية للفضاء الرقمي عدة مراحل بدءا من محاولات اختراق البيانات الرقمية المعادية و التي بدت كمحاولات منفردة لقرصنة المواقع المعادية و شبكات الأنظمة الحيوية.و في خطوة ثانية تم استخدام الشبكات الإجتماعية بغرض تبادل الاتهامات و نشر الشائعات وذلك بإشراك الفواعل المتعددة وصولا إلى تبني العسكرة الرقمية كمنهج حرب جديد و ذلك بوضع استراتيجيات سيبيرانية و استحداث قيادات عسكرية رقمية خاصة و اعتماد هياكل خاصة في و حتى انشاء جيوش سيبيرانية كاملة.

العسكرة الالكترونية :يطلق مصطلح الكتروني على الاستخدامات المختلفة لجهاز الحاسوب. والعسكرة الالكترونية تشمل جميع التطبيقات العسكرية للفضاء الالكتروني. ورغم اشتراك التعريف مع مصطلح الحرب الالكترونية وتداخله في أحيان كثيرة معها، [4]الا أن االعسكرة

---

[1]-- محمد عزت عبد الرحيم ،عسكرة المعلومات :كيف سيطر الجيش الاسرائيلي على مواقع التواصل الاجتماعي ، تقديم لكتاب العسكرة الرقمية ،لايدي كونتسمان و ريبيكا شتاين(مركز الروابط للبحوث و الدراسات الاستراتيجية،13جويلية 2015)أطلع عليه بتاريخ 16 فيفري2018
http://rawabetcenter.com/archives/94

[2] -زياد منى ،"العسكرة الرقمية "،موقع أنثربوروس(2015)،اطلع عليه بتاريخ03 مارس 2018
http://www.aranthropos.com/

[3] - Militarisme ,wikipedia(2018), dernière modification le 13 juin 2018
https://fr.wikipedia.org/wiki/Militarisme

[4] - ايمان الحياري،"مفهوم الحرب الالكترونية "،موضوع،(2016)آخر تحديث 22 ديسمبر 2016
http://mawdoo3.com/مفهوم-الحرب-الالكترونية

الالكترونية تتضمن الاستخدام غير السلمي لأدوات الفضاء الالكتروني من طرف الفواعل في المجتمع الدولي وليست حكرا فقط على الحرب والتي تختص بادارتها الدول.

العسكرة السيبرانية :لا يوجد فرق واضح سوى أن كلمة سيبيراني تعني "ترابط حواسيب مع أنظمة أوتوماتيكية "، فالنظم السيبرانية المركزية تنسق كل الآلات و المعدات التي تستخدم في المدينة الواحدة و الأمة الواحدة [1]و العالم بشكل أشمل ،و ان كانت كلمة سيبرانية هي الأقرب معنى للرقمية من الالكترونية والتي قد تعني العسكرة الحديثة التي تهتم بالوسائل والمعدات الحربية الالكترونية المختلفة كأنظمة الرادار و اللاسلكي و الاستطلاع الالكتروني و الاعاقة الالكترونية[2] وما إلى ذلك من وسائل الجيوش الذكية ، غير أن كلمة سيبرانية أشمل وأعم فهي تعني عسكرة الأدوات التي تعتمد على الانترنت والتي تعمل في شبكة عالمية تتخذ من الفضاء السيبراني مسرحا لها .

حرب المعلومات: كثيرا ما يتقاطع المصطلحين العسكرة الرقمية و حرب المعلومات ببعضهما البعض بسبب كون حرب المعلومات مصطلح جزئي[3] تتمحور حوله عملية العسكرة الرقمية ،اذ يتم خوضها للحصول على ميزة تنافسية على العدو، وقد تتضمن حرب المعلومات جمع المعلومات الاستراتيجية الموجودة، نشر الدعايات أو المعلومات الخاطئة لإحباط العدو أو الشعب والتقليل من نوعية المعلومات الموجودة لدى العدو و العمل على تقليص فرص جمع العدو للمعلومات في الوقت نفسه.[4] .

وتدخل في اطار حرب المعلومات مفاهيم ثانوية تعتبر وسائلا وأدواتا تتخذها العسكرة الرقمية لتحقيق أهدافها المسطرة كالحرب النفسية الالكترونية والتي تعني كل "نشاط اتصالي منظم يهدف إلى التأثير في توجهات و ادراكات الفاعلين الرسميين و غير الرسميين في دولة ما باستخدام الفضاء الرقمي وتكنلوجيا الإتصالات الحديثة "[5].

القوة الالكترونية :وهي القدرة على تحقيق الأهداف المرجوة من خلال استخدام مصادر المعلومات المرتبطة **ب**المعلومات وهو مصطلح يستخدم لوصف استخدام و إدارة المعلومات بالفضاء السيبراني،[6] ويشكل مفهوم القوة لب العسكرة الرقمية و الذي يعبر عن كافة النشاطات

---

[1] - "ما هي السيبرانية ؟ و ما هو دورها في صناعة القرار،زايتجايست و مشروع فينوس(2012)آخر تعديل26 ديسمبر2012
http://www.zeitgeistarabia.com/2012/12/cybernation.html

[2]، "الحرب الالكترونية :نشأتها وتطورها ومفهومها،موسوعة المقاتل" أطلع عليه بتاريخ 13 مارس 2018
http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec03.doc_cvt.htm

[3]-Ibid, " cyberguerre :concept,état d’avencement et limites"

[4] -"حرب المعلومات "،موسوعة ويكيبيديا(2017)،آخر تعديل 09 ديسمبر2017
https://ar.wikipedia.org/wiki/حرب_المعلومات

2-ريهام عبد الرحمان رشاد العباسي،"أثر الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية ،دراسة حالة :تنظيم الدولة الاسلامية"،المركز الديموقراطي العربي، (2016)آخر تحديث 24 جويلية 2016
https://democraticac.de/?p=34528

3- يوسف عبد الغني حجاج البري ، "نشأة وتطور حرب المعلومات "، مؤتمر حروب الفضاء السيبراني(2015)،آخر تعديل 15 ماي 2015https://seconf.wordpress.com/2015/05/15/ نشأة -و تطور- حرب -المعلومات

العسكرية الدائرة على ساحة الفضاء الرقمي بدءا من الدعاية و التشهير وصولا للهجومات و الاعتداءات التخريبية و تجدر الاشارة إلى أننا نفضل استخدام مصطلحات الرقمية والسيبرانية لكونها تدل بدقة على النشاطات الافتراضية التي تتصل بشبكة الانترنت و التي تمثل جوهر بحثنا هذا.

المطلب الثاني: جذور و نشأة العسكرة الرقمية

- أولا: جذور العسكرة الرقمية:

رغم أن العسكرة الرقمية ترتبط بظهور الانترنت أساسا الا أن توظيف الإتصالات و المعلومات في الصراعات الدولية يعود لما قبل الحرب العالمية الأولى ،أي منذ أن بدأت الإتصالات بين أرجاء المعمورة كافة باستخدام المواصلات السلكية عن طريق جهاز المورس"جهاز البرق الصوتي"عام 1837 عندها بدأ التفكير في استغلال الأمر عسكريا و هو ما تحقق إبان الحرب الأهلية الأمريكية 1861 أين تم استهداف خطوط التلغراف من قبل القوات المتحاربة، و قد كان لظهور الاتصال اللاسلكي بالغ الأثر في بدء عمليات الشوشرة و التشويش على خطوط الإتصالات المعادية بغرض إرباكها و شل سيطرتها على قواتها و أسلحتها، و لهذا عملت الدول خاصة خلال الحربين العالميتين على إخفاء اتصالاتها قدر الامكان عن طريق تقليل فترات استخدام اللاسلكي بسبب المراقبة، و قد كانت الحاجة العسكرية لتصحيح نيران المدفعية و إرسال التقارير من أراضي المعارك [1]و انجاز العمليات الاستطلاعية أثر هام على تحديد مسألة حسم المعارك، و رغم تطور أدوات الاتصال التي لعبت دورا حاسما في الانتصار في المعارك التقليدية الأرضية كالرادار الا أن الحاجة الماسة لتأمين طرق اتصال دائمة مأمونة و مضمونة حتى في حالة الحروب الكبرى أدت إلى مواصلة التجارب البحثية حتى التوصل الى اختراع الانترنت.

ثانيا : نشأة العسكرة الرقمية

- اختراع الأنترنت: ان بدايات اختراع الانترنت كانت منذ ما يربو عن خمسين عاما في الولايات المتحدة الأمريكية،أين اتخذ كسلاح يستخدم في اطار الحرب الباردة الدائرة بين المعسكرين الشرقي و الغربي كردة فعل لاطلاق الاتحاد السوفياتي عام 1957 لأول قمر صناعي "سبوتنيك" إلى الفضاء الخارجي، ففي ذروة سباق التسلح الدائر شعر الأمريكيون بالذعر من خسارتهم الوشيكة و ترجمت تلك الحاجة الملحة لتطوير وسيلة تستخدم من طرف الباحثين و العلماء من أجل تبادل المعلومات و البيانات من مكان إلى آخر في سرية تامة في الانترنت الذي بات يستخدم في كل مكان من العالم اليوم. ومذاك أخذ الأمريكيون الأمر على محمل الجد إذ بدؤوا يهتمون بالعلوم بمختلف أنواعها و أضافت المدارس الأمريكية مواد كالكيمياء و الفيزياء و التفاضل[2] و بدأت الحكومة بتشجيع البحث العلمي و الاستثمار فيه و تمويل مؤسساته و عمدت الحكومة الفدرالية لتأسيس

---

[1] -"الحرب الالكترونية "،مرجع سابق

[2] --- محمود كيشك ،"الحرب الباردة ...السبب الأول في اختراع الانترنت "،جورناس (2012)آخر تعديل 03 فيفري 2012
Journas .com /-KoshkAlmady/post/44490/ الحرب-الباردة – السبب- الأول –في – اختراع - الانترنت

وكالات جديدة مثل وكالة ناسا للفضاء ووكالة المشاريع البحثية المتقدمة "ARPA" بغرض تطوير أسلحة و صواريخ و حواسب آلية . وقد عبرت كل هذه الاجراءات عن القلق الشديد ازاء تعرض الولايات المتحدة لهجوم سوفياتي على شبكة الهاتف يشل تحركها بعد أن تبين أن تأمين الاتصال يتخذ أولوية قصوى خاصة و أن بامكان صاروخ واحد أن يدمر شبكة كاملة من التواصل و المسافات طويلة و تمكن العالم ليكليدز في عام 1962 من توفير حل لتلك المشكلة من خلال استحداث شبكة تحت اسم Galactic Network استطاعت الربط بين مجموعتين من الحواسب الآلية التي تمكن المسؤولين من التواصل بشكل آمن و فعال حتى في حال تدمير شبكة الهاتف. كما تمكن عام 1965 عالم آخر من معهد مساتشوستس للتكنولوجيا من تطور تقنية خاصة بنقل المعلومات الرقمية على الشبكات عرفت باسم"تحويل الطرود" إذ يتم إرسال البيانات بعد تقسيمها إلى مجموعة من الطرود"Packet Swiching" و قد استطاعت هذه التقنية إرسال تلك الطرود من ظروف مختلفة للمستقبل دون أن تكون بترتيب محدد، وهكذا استطاعت شبكة الحواسب الحكومية المعروفة "Arranet" أن تحمي نفسها من أي هجمات محتملة. وقد تم إرسال أول رسالة عبر شبكة "Arpanet" من جهاز يقع في مختبر للأبحاث بجامعة كاليفورنيا إلى جهاز آخر بجامعة ستانفورد وكان كل جهاز فيهم بحجم غرفة صغيرة و حملت وقتها كلمة "LOGIN" وكانت صغيرة جدا الا أن الشبكة تحطمت ولم يصل الا أول حرفين فقط . ومع نهاية عام 1969 تم التمكن من ربط أربعة أجهزة بالشبكة[1] واستمر الأمر بالتطور مع الوقت حتى وصلت الأنترنت إلى ما هي عليه في الوقت الحاضر.

[1] - كيشك،"الحربالباردة"،مرجع سابق

المطلب الثالث: العسكرة الرقمية:عناصرو أنماط و خصائص

كغيرها من أنماط العسكرة المعروفة عبر التاريخ اتخذت العسكرة الرقمية أنماطا و خصائصا ميزتها عن نظيراتهامن أنواع العسكرة التقليدية، استقت عناصرها من الفضاء السيبراني الذي شكل البيئة العامة التي تدور في فلكها العسكرة الرقمية .

أولا: عناصر العسكرة الرقمية

- **العنصر البشري:** ويشمل هذا العنصر كل المتخصصين في المجال الألكتروني من مهندسين و تقنيين و مبرمجين.

- **العنصر المادي:** أجهزة الكمبيوتر.

- **العنصر المعرفي:** شبكات الاتصال الداخلية "Local Area Network" والعالمية "Wide Area Network" وتتمثل الأولى في مجموعة أجهزة الكمبيوتر و التي ترتبط مع بعضها البعض عن طريق كمبيوتر رئيسي تأخذ منه المعلومات الرئيسية " Server" أي ملقم الشبكة كما هو معمول به في المؤسسات التجارية و الشركات و أجهزة الدولة، و الثانية غير مقيدة بحدود من حيث الامتداد فهي خيوط عنكبوتية يرمز لها "www" و يقصد منه "World Wide Wed" و هذه الثانية هي المعنية بالاستخدام غير السلمي كونها سهلة الاستخدام و ضعيفة الرقابة مع عدم وجود قواعد قانونية تفرض أنماطا معينة من السلوك على صعيد الفضاء السيبراني[1].

ثانيا: أنماط العسكرة الرقمية

عملت الدول على عسكرة الفضاء الالكتروني عبر عدة أنماط:

- استخدام القدرات الهجومية و الدفاعية على صعيد الفضاء الرقمي بهدف إفساد النظم المعلوماتية و الشبكات و البنية التحتية من خلال توظيف أسلحة الكترونية من قبل الفاعلين في المجتمع الدولي.

- شن الحروب النفسية و الاعلامية من خلال حملات تسريب المعلومات مما أثر على طبيعة العلاقات الدولية .

- العمل على اختراق الأمن القومي للدول عبر سرقة الأسرار الاقتصادية و العلمية و محاولة السيطرة على الانترنت و تدمير المواقع و التجسس بما يكون له تأثيرات مدمرة في الاقتصاد والبنية التحتية بذات قوة التفجير التقليدي.

---

[1] -خليفة ،" القوة"،مرجع سابق.

- تحول الفضاء الالكتروني لمسرح نشط للأنشطة الاستخباراتية بعد توظيفه من طرف أجهزة الاستخبارات الدولية المختلفة بما ساهم في دعم قدرة الأجهزة الأمنية للدول أو حتى الجماعات المختلفة على تشكيل شبكة عالمية من العملاء بدون تورط مباشر[1].

ثالثا:خصائص العسكرة الرقمية :

بفضل الفضاء السيبراني تحولت العسكرة الرقمية الحديثة من مفهوم استاتيكي جامد يرتبط بالجغرافيا و التاريخ و الجيواسترتيجية إلى مفهوم ديناميكي متغير و متغلغل في كل مناحي الحياة ليرتبط بالانسان في حد ذاته .فقد أعطت العسكرة الرقمية بعدا جديدا للسيطرة و التي تحولت من امتلاك القوة إلى السيطرة على الأفكار و امتلاك السياسات و هو الأمر الذي ميز العسكرة الرقمية وصنع الفرق بينها و بين العسكرة التقليدية.

- **تغير الأهداف و الوسائل:** ان انعدام القدرة على الحسم العسكري في الحروب التقليدية تطلب التحول من عسكرة تقليدية تعتمد على ضمانة الترسانة المادية التقليدية إلى عسكرة رقمية الكترونية بسبب "تغير برادايم الحرب جذريا و انتقاله من نسق الحروب فيما بين الدول إلى نسق الحروب في وسط الشعوب"[2] ففي حين كان الهدف قديما هو تدمير العدو و ذلك باحتلال أرضه و الاستيلاء على موارده أصبح اليوم هو التحكم في إرادته و خياراته ومن هنا برز الدور المحوري للشعوب في هذا الصنف الجديد من العسكرة بعد أن تصاعدت أهمية دور الرأي العام المحلي أو الرأي العام الاقليمي و الدولي.
- **تغير طبيعة التهديد:** أصبح التهديد دائما و غير مباشرا ومحتملا بما حول النزاعات المؤقتة لصراعات مستمرة بسبب سهولة الاستهداف.
- **طبيعة الاستهداف الدائمة :**عدم قدرة الدولة على الحركة و التدخل للسيطرة على التفاعلات الجارية على صعيد الفضاء الرقمي أسفر عن حالة عجز كان مردها عدم قدرتها تمييز المصادر الداخلية عن الخارجية و بالتالي ضعف سيطرة أنظمة الحكم على توجهات مواطنيها.
- **تغير نمط الصراع:**تحول الصراع من صراع دموي إلى صراع نظيف فلا ترافقه دماء و أشلاء بل يتضمن التجسس و التسلل إلى مواقع الخصوم الرقمية و قرصنتها. هذا التوجه نحو نمط "الحروب النظيفة"مرده مآسي الحرب العالميتين و صعوبة التلويح بحرب نووية ثالثة مما أدى لتنامي التوجه نحو استغلال التفوق التقني الاعلامي و العسكري بغرض حسم حروب تجنب السكان مآسي المواجهة المباشرة لذا فان استغلال الفواعل لخصائص الشبكات الالكترونية تنوعت إستراتيجيتها في استخدام هذه الميزات التقنية و ذلك بإتباع المواجهة المتدرجة التي تسعى لانهاك الخصم و التسلل إلى وسط السكان و زعزعة ثقتهم في مؤسسات الدولة بغرض تحويلهم لأرضية مواجهة بديلة باستعمال سلاح الصورة و شحن الرأي العام.وقد برز هذا بقوة في تبني فكرة إسقاط النظام من الداخل بدلا من استخدام القوة العسكرية .

---

[1] - عبد الصادق ،"الحروب السيبرانية :تصاعد القدرات و التحديات للأمن العالمي " ،المركز العربي لأبحاث الفضاء الالكتروني(2017)آخر تحديث12 مارس 2017
http://accronline.com/article_detail.aspx?id=28395

[2] - عبد الصادق،"الحروب السيبرانية"، مرجع سابق.

- **السرية و الغموض:** التي تطبع العسكرة الرقمية سواء من حيث الأهداف أو الوسائل أو الأطراف فعدم وضوح الأطراف المعنية بالعسكرة الرقمية خلافا للعسكرة التقليدية يؤدي لعدم تمييز الأعداء.
- **تغير نمط الاستهداف الخارجي المباشر:**واستبداله بالتحول إلى التسلل داخل قوة الخصم في محاولة لتفتيتها و شلها.
- **العسكرة الرقمية عسكرة غير فتاكة:**أي أنها ليست لها صفة مميتة [1]ففي الوقت الذي يشكل التهديد بالموت أحد معايير امتلاك السلاح التقليدي فان عسكرة الفضاء الرقمي نظيفة أولا بسبب طبيعة الأسلحة غير الفتاكة و ثانيا بسبب التوجه نحو انتهاج نمط الحروب النظيفة والتي قادت الفواعل تدريجيا لاستبدال نمط الصراع التقليدي بالفضاء الافتراضي الذي يمكن من اعداد الملايين من البيانات و المعلومات المراد توصيلها إلى الهدف المحدد بما يسمح بالتحكم بأفكاره و توجيه سلوكياته مع محاولات إضعاف معنوياته و إحباط مخططاته و هي الاستراتيجية الجديدة التي يوفرها الفضاء السيراني.

بعد أن غدت أهداف العسكرة الرقمية أقل مادية يحتل فيها العامل النفسي و الدعائي المرتبة الأعلى بسبب تزايد التغطية الاعلامية و الاخبارية المباشرة للأحداث سمعية كانت أم بصرية وذلك لحظة وقوعها إذ تبث عبر مواقع الانترنت و الفضائيات مع تسجيل ضعف سيطرة أنظمة الحكم على توجهات مواطنيها. وهو ما دفع لطرح افتراضات قد تكون خاطئة و تؤدي لخلق أعداء أو إشعال حروب فعلية دونما وجود داع لذلك.

- **عدم امكانية معاينة آثار العسكرة الرقمية:في الغالب** لا يمكن معاينة الهجمات و طبقا لتقرير صدر عام2013 وجد أن أغلب الشركات لا تستطيع معرفة ما إذا كان هناك اختراق لأنظمتها أم لا، و قد يحتاج الأمر شهورا عدة و حتى سنوات حتى تستطيع اكتشاف ذلك.
- **تعدد الفواعل :**تستم العسكرة الرقمية خلافا للتقليدية التي تعتمد على الفاعل التقليدي المتمثل في الدولة بتعدد الفواعل فبالاضافة إلى هذه الأخيرة الدولة برز دور الأفراد و الجماعات و الشركات في تفعيل الفعل العسكري.[2]
- **البعد الأخلاقي:** رغم أن المشكل الأخلاقي مطروح في كلتا العسكرتين :التقليدية و الرقمية الأ أن غياب البعد الأخلاقي حاضر بشدة كون أن الأسلحة الرقمية تتميز بعدم تميزها للأهداف المدنية من العسكرية،كما أن الصراع الذي تديره العسكرة الرقمية يتصف بغياب قواعد واضحة ومحددة للاشتباك أو وقف القتال. وتتعلق معظم هذه الخصائص بمتغير القوة الالكترونية الذي شكل العلامة الفارقة للعسكرة الرقمية.

ترتكز عناصر القوة السيبرانية على وجود نظام متماسك بين القدرات التكنولوجية و السكانية و الاقتصادية و الصناعية و القوة العسكرية وإرادة الدولة و غيرها بما يسهم في دعم إمكانات الدولة على ممارسة الاكراه و الاقناع أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم و السيطرة على الفضاء الالكتروني. و يعمل ميكانيزم القوة السيبرانية باتجاهين:

---

[1] -،مرجع سابق.
[2] - عبد الصادق ،"الحروب السيبرانية "،مرجع سابق.

- أولا:تدعيم القوة الناعمة للدول بشن الهجمات التخريبية و ذلك عن طريق نشر المعلومات المضللة و الحرب النفسية و التأثير في توجهات الرأي العام و التجسس.[1]

ثانيا:تبني سياسة دفاع الكتروني تقوم بحماية الشبكات الوطنية من خطر التهديدات و ذلك ببناء مؤسسات وطنية للحماية الالكترونية عن طريق رصد ميزانيات كبيرة. وبدا جليا أن الذي يدير العالم آحاد و أصفار فمن يمتلك توظيف البيئة الألكترونية هو الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة. [2]

[1] - الصباحي ،"أبعاد القوة "،مرجع سابق

[2] - محمد الحمامصي ، " حروب العصر الافتراضي :تغير مفاهيم القوة و التوازنات العالمية"، العرب(2017)،
آخر تحديث 17 أفريل 2017
https://alarab.co.uk/حروب -العصر – الافتراضي -تغير مفاهيم -القوة -والتوازنات - العالمية

[2] -Ibid, "Cyberguerre :concept,état d'avencement et limites "

المبحث الثالث: وسائل وأشكال و آليات العسكرة الرقمية

المطلب الأول: وسائل العسكرة الرقمية:

أولا:الأسلحة الالكترونية:

سلاح الأنترنت معروف تحت مصطلح القدرة اذا تسمى قدرات الأنترنت "zero days" و القدرات الالكترونية كأسلحة تختلف بطرق رئيسية عن الأسلحة التقليدية كالصواريخ و القنابل فهي أولا:

- تسبب أضرار أقل علانية و لكن أكثر انتشارا من الهجوم المادي، إذ يمكن للهجوم بالسلاح الالكتروني أن يشل الاقتصاد المحلي في دولة كالبرتغال مثلا.

- إمكانية شن هجوم فوري مباغت ضد أي هدف في العالم.

- الانترنت تلغي المسافة المادية بين الأعداء.

- عدم مرئية الأسلحة الرقمية يجعل منها أسلحة فتاكة بسبب عدم إمكانية رصدها.

وتتنوع أسلحة الهجوم الرقمي بين:

1- **الفيروسات:** تستخدم لضرب شبكات الخدمات و البنية التحتية وهي معروفة في كل بيئة مبنية على استخدام الكمبيوتر و بإمكانها احداث شلل كلي لشبكة الإتصالات في الدولة طالما كانت الشبكة مؤسسة على الحاسب الآلي مثلما حدث ذلك مع نظام شركة at&t الأمريكية في 15 يناير سنة[1] 1995. و الفيروس برنامج له آثار تدميرية على أجهزة الحاسوب بسبب قدرته الفائقة على التخفي فهو يقوم بنسخ نفسه أكثر من مرة وهي العملية التي تجعل ملفاته المفتوحة تحل محل الملفات الأصلية الموجود على القرص الصلب hard disk للحاسوب.
2- **الديدان:تمثل** الدورة برنامجا مستقلا يتكاثر بنسخ نفسه عن طريق الشبكات[2] و تستهدف تدمير البيانات و قطع الإتصالات نظرا لقدراتها الكبيرة في تغيير شكلهاأ وقد أختير لفظ worm باللغة الانجليزية أي دودة أو أفعى يتم استخدامها في استهداف الشبكات المالية المؤسسة على الكمبيوتر مثل شبكات البنوك و البورصات.
3- **أحصنة طروادة "Trojan Horse":**وهو برنامج صغير أو جزء من شفرة يختبئ في برنامج أكبر منه عادة يكون برنامجا شهيراً و ذائعا،تتمثل وظيفته في تأدية مهام خفيفة كإطلاق فيروس أو دودة كما يقوم بمسح آثاره التي تحمل صفة تخريبية، لذلك فأحصنة طروادة المبرمجة بمهارة لا يمكن اكتشاف وجودها، و يتركز دورها أساسا في إضعاف بيئة الخصم قبل اندلاع المعركة اذ يقوم بتحديد الثغرات لنظام ما و قرصنة كلمات المرور السرية الخاصة به[3].

---

[1] - " أسلحة حرب المعلومات و استخداماتها" ،أرشيف إسلام أون لاين ،أطلع عليه في 04 ماي 2018
00https://archive.islamonline.net/?p=982
.

1- الصباحي، أبعاد القوة"،مرجع سابق.

4- **القنابل المنطقية "Logic bombs":** [1] و تعد نوعا من أنواع أحصنة طروادة تزرع داخل النظام أو تكون برنامجا مستقلا و تستخدم بغرض التلصص و التجسس و تحليل موقف الدول المعادية.

5- **الأبواب الخلفية "Back doors":** وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إلى النظام عند الحاجة و هنا يجب لفت النظر إلى الدور الذي يلعبه منتجو البرامج و الأنظمة في اختراق الحاجز الأمني للدول، و تجدر الاشارة إلى أن كل البرامج و النظم التي تنتجها الولايات المتحدة تحتوي على أبواب خلفية يتم استخدامها عند الحاجة وهو ما يمكن هيئات و أركان حرب المعلومات من التجوال الحر داخل أي نظام لأي دولة أجنبية كانت.

6- **مدافع AERF و قنابل EMP:**

تطلق مدافع HERF موجات راديوم مركزة و عالية الطاقة و التردد high energy radio freqency يمكنها تعطيل و إتلاف أي هدف الكتروني. و تتراوح الأضرار بين أضرار توصف بالمتوسطة تتمثل غلق شبكة الحاسوب او اعادة تشغيله بشكل دوري مما يمنع عملية استغلاله، أو أضرار بالغة كإتلاف العتاد الخاص بالحاسوب أو الشبكة بشكل لا يمكن معه إصلاحهما. وتشبه قنابل emb المدافع لكنها تستخدم نبضات الكترو مغناطيسية electro magnetic بما يمكن من التسلل إلى مواقع العدو الالكترونية الحساسة و الهامة وإلقاءها بغرض اتلاف كل الحواسب و الشبكات في دائرة انفجارها الغير مرئي. ورغم صغر حجمها عن مدافع herf الا أن أثرها أبعد حيث لا يمكن لها تحديد هدفها بينما تنتقي قذيفة مدفع herf هدفها بدقة. و تولي الدول أهمية كبيرة لهذا النوع من الأسلحة السيبرانية لما تخلفه من آثار بالغة الدمار.

7- **الرقائق" Chipping "**

من المعروف أن للبرنامج و النظم software وظائف غير معروفة أو غير متوقعة و هو الأمر الذي يسير بالمثل فيما يخص الرقائق إذا يمكن للدوائر المجتمعة IC's و التي تشكل هذه الرقائق التي تحتوي على وظائف تضاف لها عند تصنيعها ميزتها، أنها لا تعمل في الظروف العادية بل تستجيب للعصيان في وقت معين أو عن طريق الاتصال بها عن بعد حيث يمكن أن تستجيب لترددات معينة كبعض موجات الراديو فتشل الحياة في المجتمع أو الدولة المعنية بالاعتداء[2].

8- **الماكينات و الميكروبات فائقة الصغر:** ويطلق عليها Nano machines and microbes على عكس الفيروسات التي تصيب برامج المعلومات فالماكينات بإمكانها إصابة عتاد النظام نفسه nano machines hardware ،تمثل روبوتات robots فائقة الصغر تنتشر في بنية النظام المعلوماتي للدولة المعادية منقبة عن حاسب آلي تدخل إليه من خلال الفتحات الموجودة به و تقوم بإتلاف الدوائر الالكترونية. أما الميكروبات فبما أنها تتغذى على الزيت يتم تحويلها جينيا لتتغذى

---

2 - نوران شفيق ،اثر التهديدات الالكترونية على العلاقات الدولية:دراسة في أبعاد الامن الالكتروني(المكتب العربي للمعارف)،28،أطلع عليه بتاريخ15 أفريل2018
https://books.google.dz/books?id=r7dQDwAAQBAJ&pg=PP1&lpg=PP1&dqsource=bl&ots=ZuS6WuCNMs&sig=9tuIy7onRweyQOerdZD0tk0Cd

[2] - الصباحي، مرجع سابق .
2- "أسلحة حرب المعلومات "،مرجع سابق.

على عنصر silizium و هو مكون هام في الدوائر الالكترونية يعمل على تدمير و إتلاف الدوائر الالكترونية لأي معمل يتوفر على حاسبات آلية أو حاسب خادم server لموقع على الانترنت أو أي مبنى يدار بالكمبيوتر ويصل إلى إتلاف المرافق الحيوية لمدينة بكاملها[1].
10-الاختناق المروري الالكتروني**:** تم تطوير طريقة سد و خنق قنوات الاتصال لدى العدو حتى يتم منعه من تبادل المعلومات فيما يسمى electronic jomming تم تطوير هذه الطريقة بعملية استبدال المعلومات بمعلومات زائفة و هي طريقها بين المستقبل و المرسل.

ثانيا: الهاكرز والكراكرز:

تحمل كلمة "Hackers" معنى يختلف تماما عما تحمله هذه الأيام فقد بدأت كصفة تشير إلى عبقرية مبرمجي الكمبيوتر و قدرتهم على ابتكار أنظمة و برامج حاسوب أكثر سرعة و من أشهر من ألصقت عليه هذه الصفة " دينيس ريتش" و " كييف تومسون" اللذان صمما برامج البرونكس عام 1969 أما الهاكرز بالمفهوم السيئ فلم يكن لهم وجود قبل سنة 1981 و هي السنة التي شهدت ظهور أول حاسوب شخصي من انتاج شركة IBM، ذلك أن عمليات القرصنة كانت بغاية الصعوبة لعدة أسباب منها أن أولى النسخ من الحواسيب كانت كبيرة جدا بل ضخمة و تحتاج لغرف كبيرة تتوفر على درجات حرارة ثابتة و قد اقتصرت أشكال انتهاك خصوصية الآخرين على التنصت على هواتف الغير من خلال شركات الهواتف المحلية كما اتخذت شكل التلصص على أسرار الناس و ابتزازهم وقد يستلزم الأمر شهورا لاصلاح الأضرار التي يتسبب بها الهاكر لسد الثغرات التي ساهم في توسيعها هذا دون ذكر الخسائر المادية الكبيرة.

و يرد هنا ما أحدثه أحد مشاهير الهاكرز: روبرت موريس سنة 1988 حيث عندما قام بتطوير أفعى اليونيكس مما تسبب في تعطيل ما بين 15 إلى 600 مليون جهاز حاسوب أي ما يوازي عشر أجهزة الانترنت في ذلك الوقت[2]. و قد قدرت الخسائر المادية حينها ما بين 15 إلى 100 مليون دولار و يعمل الهاكرز عادة فرادى كما يسجل تجمع بعضهم في مجموعات صغيرة ليقوموا بالقرصنة الالكترونية، غير أن هذه المجموعات عادة ما يكتشف أمرها بسبب تجمعها على هدف واحد أو قضية معينة مما يسهل عملية تعقبها كالقراصنة الكوبيون و المجريون و حتى البلغار و البرازليون الذين تعاطفوا مع هاكرز عرب و قاموا بالتعاون لاغلاق عشرات المواقع الاسرائيلية ردا على ما تمارسه سياسة الاحتلال في الأراضي الفلسطينية ووصل الأمر حد طلب الحكومة الاسرائيلية منهم وقف النار في معركة قصف مواقع الانترنت المتبادلة بينهم بسبب الأضرار الكبيرة التي لحقت بالكمبيوتر والتي انعكست سلبا على أداء المؤسسات الرسمية الاسرائيلية فضلا عن ضرب السمعة الدولية و التجارية للحواسيب[3].

الكراكرز: تطور الأمر باستخدام شبكة الانترنت للاعتماد على برامج التجسس فأخذ الهاكرز الجدد بزرع الملفات التجسسية" patch tronans" في حواسيب الضحايا عن طريق البريد الالكتروني الخاص بهم أو باستغلال ثغرات الوندوز التي تكتشفها البرامج التجسسي و اقتصر نشاطهم في

---

[2] -"أشهر هاكرز على مستوى العالم "،ساسة بوست(2014)،آخر تحديث 08 أكتوبر 2014
https://www.sasapost.com/hackers/

[3] -"مخترق"،موسوعة ويكيبيديا(2018)،آخر تعديل 17 جوان 2018
https://ar.wikipedia.org/wiki/مخترق

البداية على سرقة البريد الالكتروني و التلاعب في هذه الأجهزة . و كانت هذه العملية تشير الى النوع الأول من الفواعل والذي يعبر عنهم بالهاكرز الهواة.

أما النوع الثاني من الهاكرز و هم المحترفون فيدعون بالكراكرز ، فبالاضافة إلى استخدامهم للبرامج الجاهزة و المتطورة فانهم يستخدمون ما لديهم من علم و يهتمون بتطويره إذ يعتمدون على خبرتهم في لغات البرمجة و التشغيل في تصميم و تحليل البرامج، و قد استطاع الهاكرز اختراق شركة مايكروسفت و وزارة الدفاع الأمريكية و وكالة نازا للأبحاث. و تكمن خطورة الهاكرز بأن نجاح عملية تسلل واحد منهم إلى أنظمة الكمبيوتر الحكومية مثلا لمدة نصف ساعة تستلزم 24 ساعة على الأقل لتقدير لمعرفة و اكتشاف حجم الأضرار. .[1]

ثالثا: الأنونيموس: Anonymous

اسم يطلق على عدد من المستخدمين المجهولين للانترنت و يمثل المصطلح أعضاء ثقافة أنترنت معينة. و تحديدا فالأنونيموس مجموعة قليلة تعمل في مجال النضال عبر الاختراق البرمجي، وجدت عام 2003 على منتدى الصور ' 4 تشان' تمثل مفهوما لمستخدمي شبكة الأنترنت غير موجودين في مكان واحد و لكن يطلق عليهم مجازا مجتمعا أنترنتيا.

كما يعتبر مصطلحا مبطنا لأعضاء من جماعات اجتماعية منعزلين في شبكة الانترنت يتفقون على هدف واحد قاموا باختراق العديد من المواقع الحكومية و أنشطة الحاسوب لأهم شركات الحماية الالكترونية.

و يعد الأنونيموس أنفسهم مقاتلين رقميين و حسب تصنيف شبكة سي أن أن CNN عام 2012 فانهم يعتبرون من أكثر الجماعات تأثيرا في العالم[2]، و قد كانت بدايتهم عن طريق شبكة

لامركزية تصرفوا فيها بشكل مجهول و منسق نحو هدف ذاتي و يتخذ أفراد الجماعة أقنعة يخفون بها وجودهم عند مواجهتهم لوسائل الاعلام.[3]

رابعا: التسريبات

1- **تسريبات ويكيليكس**:

تنسب التسريبات الشهيرة لمنظمة ويكيليكس و هي منظمة دولة غير ربحية عمل موقعها على الانترنت منذ سنة 2006 على نشر التقارير الخاصة السرية تحت مسمى منظمة سن شاين الصحفية، وقد اهتز الرأي العالمي إثر نشرها ل90 ألف ثم 400 ألف وثيقة نسبت للبنتاغون ثم 250 ألف مستند نسب للخارجية الأمريكية. كما فضحت تسريبات الويكيليكس ممارسات الحكومة الأمريكية في معتقل غوانتانامو ووحشية القوات الأمريكية و هي تقتل مدنين من بينهم صحفيين من وكالة رويترز الاخبارية في أحد أحياء بغداد سنة 2007.

---

[1] -"مخترق"، مرجع سابق
https://ar.wikipedia.org/wiki/ مخترق
[2] - "الانونيموس"،موسوعة ويكيبيديا(2018)،آخر تعديل 20 جوان 2018
https://ar.wikipedia.org/wiki/ أنونيموس-_(مجموعة)

و نشرت وكيليكيس وثائق عن عمليات قتل و إعدام للمدنيين في العراق و أفغانستان كما كشفت عن عضوية عدد من ضباط الجيش و الشرطة البريطانيين في الحزب القومي البريطاني.

و رغم ما قيل عن التسريبات المتعمدة الا أن فضحها لعمليات التجسس التي قامت بها الولايات المتحدة على حلفاءها الأوربيين زاد من مصداقية مصادر معلوماتها و استمرت سلسة الفضائح رغم التهديدات التي تلقتها من البنتاغون.

وقد عملت التسريبات على فضح الدور الايراني في العراق ولفت الأنظار له و لخطورته على أمن المنطقة كم أشارت إلى اتخاذ الحكومة الأمريكية لسفاراتها حول العالم كقواعد تجسس تنطلق منها عملياتها الاستخباراتية[1]. وساهم موقع ويكيليكس برئاسة مؤسسة " جوليان أسانج" الأسترالي الجنسية في تعميم نمط المنصات التي تنشر المعلومات السرية على الأنترنت في العالم .

.

و رغم ما أثارته تسريبات الويكيليكس من مخاوف البلدان بشأن نشاطاتها و على رأسها الولايات المتحدة الا أنه لوحظ عدم تسريب أية ممارسات إسرائيلية على موقع المنظمة و قد اتخذ أسانج من سفارة الأكوادور بلندن مقرا له بعد حملة التهديدات المتوالية على موقعه[2].

2- **تسريبات سنودن**:

قام العميل الأمريكي لدى وكالة المخابرات المركزية و المتعاقد التقني لدى وكالة الأمن القومي ادوارد جوزيف سنودن**Edward** Joseph **Snowden** بتسريب معلومات سرية للصحف و الفرار بعدها إلى الخارج أين استمر بحملة تسريبات واسعة دامت لسنوات، وقد واجه ادوارد سنودن المولود في 21 جوان 1983 عدة إتهامات سنة 2013 من بينها التجسس و سرقة ممتلكات حكومية و نقل معلومات خاصة بالدفاع الوطني دون ترخيص اثر تسريبه لأسرار برنامج

بريزيم" **PRISM** " إلى صحيفة الغارديان و واشنطن بوست و لجوءه إلى روسيا بعد أن طالبت الولايات المتحدة الأمريكية من هونغ كونغ تسليمها له إثر فراره لها أولا.

و قد كان من أهم و أخطر ما سربه العميل سنودن هو الميزانية المفصلة[3] لجميع وكالات الاستخبارات الأمريكية و المسماة بالميزانية السوداء و التي أتاح نشرها لمنافسي الولايات المتحدة باتخاذ الاجراءات و الاحتياطات اللازمة ضد التدابير الأمريكية، و لا تنفك تداعيات هذه التسريبات تتفاقم منذ أن رفض سنودن محاولات الحكومة الأمريكية العفو عنه مقابل توقيف نشر الوثائق السرية الخاصة بالأمن القومي الأمريكي.

1- "هل تعرف معنى ويكيليكس ولماذا يعيش مؤسسه في سفارة منذ 4 أعوام"،ملفات ويكيليكس و بنما السرية(113) ، سبوتنيك(2016)،آخر تحديث 02 أكتوبر2016

https://arabic.sputniknews.com/art/201610021020317067- تسريب-وثائق-أسانج-ويكيليكس/

[2] -"هل تعرف معنى ويكيليكس"،مرجع سابق.

[3] -"تسريبات سنودن الأخطر في تاريخ أميركا"،سكاي نيوز ،(2013) آخر تعديل26 أكتوبر 2013
تسريبات - سنودن- الاخطر- في – تاريخ - أمريكا https://www..skynewsarabia.com/461551 .

حيث كشفت التسريبات عن تجسس الولايات المتحدة على عدد من الدول مما أضر بعلاقاتها خاصة مع الدول الحليفة منها، فقد فضحت تسريبات سنودن تنصت وكالة الاستخبارات الأمريكية على الهواتف المحمولة لعدد لا يستهان به من رؤساء و وزارء الدول الأوروبية كالمستشارة الألمانية أنجيلا ميركل و رئيسة البرازيل ديلما روسيف و رئيس المكسيك السابق فيليبي كالديرون و رؤساء فرنسا المتتاليين.

ووصل عدد الزعماء المتجسس عليهم 122 شخصية.وقد خلقت هذه التسريبات ضجة كبيرة في الأوساط السياسية بعد إثبات تورط الوكالة في برنامج لجمع البيانات الضخمة إسمه "TEMPORA "[1] يدار بالتعاون مع مقر الإتصالات الحكومية البريطانية (GCGQ) .

و تكلف وكالة الأمن القومي 250 محللا لتحليل البيانات المجمعة عن طريق برنامج

"TEMPORA " الذي يمكنه الوصول لمحتوى البريد الالكتروني و مداخل الفيس بوك و سجل تصفح الانترنت[2].

و تمتد السيطرة الأمريكية حسب سنودن للقدرة للوصول للمعلومات مباشرة من أجهزة البلاك بيري و هواتف أي فون و الأندرويد حتى و هي مغلقة.

و أشارت تسريبات سنودن إلى قيام وكالة NSA بزرع برامج ضارة بالحواسيب تسمى IMPLANTS كخلايا نائمة يتم تنشيطها متى إستلزم الأمر، و أدى الأمر لاختراق أكثر من 50000 حاسوب و هو ما أكدته شركة غوغل مؤكدة أن شعار الوكالة " جمع كل شيء" لايزال ساري المفعول، فالوكالة تحصل على 200 مليون رسالة نصية كل يوم من خلال برنامج يسمى dishifire و قد تطرق سنودن إلى عمليات الاختراق التي أصابت أهدافا في هونغ كونغ و الصين أين أصابت عدة جهات حكومية و مسؤولين رفيعي المستوى ،و تمثلت أهمية تسريبات سنودن في كونها تفصيلية إذ جاء فيها شرح كيف تمت عمليات الاختراق و التي حدثت عبر الولوج إلى أجهزة توجيه الأنترنت الضخمة التي تسمح بالوصول لآلاف الحواسيب دون الحاجة لإختراق كل واحد على حدة . و أكد سنودن على قيام الوكالة بالسيطرة على الهواتف المحمولة عبر عدد من البرامج التي طورها، فعبر رسالة نصية واحدة يتم إرسالها إلى هاتف معين يتم اختراقه و تشغيل الميكروفون و الكاميرا دون علم المستخدم حتى في حالة خلوه من الطاقة.

و إستمرت الوثائق السرية المسربة تؤكد اختراق الأجهزة الحكومية الصينية و التنصت على الهواتف المشفرة و رغم سعي الوكالة لإحتواء الوضع الا أن سنودن إستمر بفضح ممارسات وكالة الأمن القومي بشأن إستخدامها لبرنامج بريزم لجمع بيانات مستخدمي مايكروسوفت و جوجل و فايسبوك و سكايب و غيرها من مواقع التواصل الإجتماعي.

---

[1] - اسراء حسني،"أخطر وثائق سربها عميل الأمن القومي الأمريكي تكشف تجسس أمريكا على العالم ..تتبع هواتف رؤساء الدول ..اختراق أجهزة حكوميةصينية ..الوصول الى مراكز بيانات جوجل وياهو..التنصت على الهواتف حتى المشفرة منها"، اليوم السابع ،آخر تعديل 06 أكتوبر2015 https://www.youm7.com/story/2015/10/23761096/ أخطر –وثائق –سربها –عميل –الأمن – القومي-تكشف-تجسس

[2] «Opération Tompora : comment les brétanniques dépassent les américains pour espionner Internet », LEXPRESS.fr(2013),22 13 2013
https://lexpansion.lexpress.fr/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_1434134.html

و عن قيامها بانشاء وحدات تكنولوجية خاصة بتحليل البيانات المسروقة ،أثبت حصول الوكالة على أمر من محكمة سرية بجمع سجلات البيانات الهاتفية اليومية من شركات الهواتف في الولايات المتحدة بغرض مساعدة المخابرات الأمريكية في تتبع اتصالات الارهابيين المشتبه بهم أو المعروفين.

و هو الأمر الذي أدى لهياج الرأي العام الأمريكي بشأن انتهاك الخصوصية و أسفر في النهاية عن إجبار الرئيس السابق باراك أوباما لإجراء تغيرات تهدف لتغيير البيانات التي تم جمعها.

و إتهم ادوارد سنودن بالخيانة[1] على حد قول الادارة الأمريكية بسبب تعريضه الأمن القومي الأمريكي للخطر و إضراره بسمعة الولايات المتحدة في الداخل و الخارج.

المطلب الثاني : آليات العسكرة الرقمية

أولا : الهجمات الرقمية

تعني الهجمات الرقمية كل " فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف ما، تمكن المهاجم من التلاعب بالنظام"[2] فاذا كان هدف أنظمة المعلومات هو اقامة المعلومات و ضمان سلامتها فالهجمات الرقمية تهدف على العكس من ذلك إلى استهلاك سريتها أو تعديلها و منع الوصول إليها.

و الهجمة الرقمية الالكترونية تتمثل في عملية ادخال برامج ضارة أو خبيثة بشكل ما إلى أجهزة الحاسوب و تثبيتها داخله دون علم المؤسسة أو الشخص المالك لهذا الجهاز بهدف الاضرار به، و تنوع الهجمات حسب الهدف المرجو منها رغم امكانية مهاجمة الأجهزة الحاسوبية حتى في حال عدم ارتباطها بالشبكة العنكبوتية كنوعية target الا أن توفر التكنولوجيا لأعداد ضخمة في العالم حال دون تمييز الهجمات ذات الأهداف المعقدة و المحصنة مثل أجهزة البنوك و الدفاع و التي تتطلب معلومات ضخمة لا يستطيع توفيرها سوى أجهزة امنية و شركات معينة تملك معلومات متقدمة في هذا المجال.

وتتنوع الهجمات السيرانية بين:

- سرقة كلمة المرور للمستخدمين للتسلل للنظام.
- هجمات رفض آداء الخدمة "انكار الخدمة (هجمات دوس dos)[3]
- القائم على الاتصال
- منقطع الاتصال
- الهجمات الطمسية.

---

[1] -مرجع سابق.

[2] - رغدة البهي، "الردع السيراني: المفهوم والاشكالية و المتطلبات"، مجلة العلوم السياسية و القانون ،العدد الأول ،المركز العربي الديموقراطي(2017)، آخر تحديث21 فيفري2017
https://democraticac.de/?p=43837

2-"هجماتosd الالكترونية" ،الباحثون السوريون(2017) ،آخر تحديث 02 نوفمبر 2017
https://www.syr-res.com/article/14290.htm

- هجمات البنية التحتية.
- قراصنة المعلومات.
- المبتدئين.[1]

رسم بياني يوضح القطاعات المستهدفة بالهجمات السيبرانية [2]



كما تم تصنيف الهجمات الرقمية لعدة أنواع هي:

- **الهجمات السرية:** و هي بمثابة نوع من أنواع التجسس التقليدي تستخدم فيه التكنولوجيا الفائقة، و تدخل ضمن هذه الفئة الهجمات السيبرانية المتطورة التي تطلقها الدول القومية أو الجماعات الاجرامية، وتكمن المعضلة في استحالة الرد بهجوم ساحق على التجسس السيبراني مهما بلغت خطورته و تداعياته على الأمن الوطني[3].

Integrity attackes- : تصمم هذه الهجمات بغرض تخريب نظم معلومات الخصم المادية و العسكرية الهامة وذلك جراء التلاعب بالبيانات داخل نظم المعلومات مّما يؤدي إلى نشر معلومات خاطئة داخل أنظمة الذكاء و اختفاء أنشطة محددة قد تكون تحت المراقبة تلبية لإستراتيجية التضليل المتعددة.

1-البهي ، الردع السيبراني"،مرجع سابق.
2-سارة عبد العزيز ،"الحرب السيبرانية :التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية "،المنهل (2018)،اطلع عليه بتاريخ 04 أفريل 2018
https://platform.almanhal.com/Files/2/100742
3-البهي ، الردع السيبراني ، مرجع سابق

Availability attackes- : وتعد من أخطر التهديدات على الأمن القومي اذ تسعى لاغلاق نظم المعلومات .

To bring information systèmes office

و تسبب الهجمات طويلة المدى منها في أضرار مدمرة للاقتصاد مثل استهدافها لشبكة الإتصالات و الكهرباء و أمّا قصيرة المدى فتهدف لجمع المعلومات الاستخباراتية الجوية[1].

و يجدر بنا التأكيد على أن فعالية العمليات السيبرانية الهجومية تلعب دوراً هاماً في التغيير الكلي لموازين القوى، و من أبرز الهجمات السيبرانية الناجحة تلك التي استهدف استونيا وجورجيا، كوريا الجنوبية و الولايات المتحدة الأمريكية .

ثانيا: حرب الشبكات Netwar :

تؤدي الميديا الإجتماعية أو وسائل التواصل الإجتماعي دوراً رياديا في عملية التضليل، حتى أنها تفوقت على وسائل الاعلام التقليدية التي تمارس نشر الأكاذيب و الأخبار المزيفة بعد أن غدت الوسائط الإجتماعية تلعب دورا هاما في التواصل بين الأفراد و الجماعات التي توظفها متى أثبتت الفائدة المرجوة منها أو منعت الضرر المراد درئه.

و من هنا كانت العلاقة بين وسائل الاتصال الإجتماعي و السياسة العسكرية للجنود و المسؤولين السياسيين و العسكريين اذ حول الفضاء الافتراضي لساحة حرب اضافية يشنها الخصوم على بعضهم البعض بل و يفاخرون علانية بانتصاراتهم الأرضية بغرض كسب المزيد من التأييد و المساندة وهو ما لمسناه في الثورات و الانتفاضات التي شهدتها البلدان العربية ابان ما سمي بالربيع العربي. كما تجد في سياسات الاحتلال الاسرائيلي التي امتدت لتشكل الفضاء الرقمي مقدما بذلك الدعم المعنوي لاحتلاله المادي للأرض.

حتى أن العسكرة الرقمية عرفت بأنها تلك الحرب التي تقودها الشبكات الإجتماعية فالحرب الرقمية تعني العملية التي استحالت عبرها منصات التواصل الرقمي[2] و الممارسات الاستهلاكية في العقديين الأولين من القرن الحالي إلى أدوات حربية في أيدي الفاعلين[3] بعد أن كانت أدوات ترفيهية و نقل للمعلومات تسعى الدول و الجماعات المختلفة للسيطرة عليها بغرض استمالة الرأي العام العالمي الذي أظهر تفاعله مع هذا الوسيط التكنولوجي الجديد، و لا تتوفر لحد الآن وسيلة ناجحة لمواجهة مثل هذه التكنولوجيا التي باتت تهدد الاستقرار و الأمن الإجتماعي و السياسي بالنظر إلى أن خدمات وسائل التواصل الإجتماعي مثل فيسبوك و تويتر و أنستغرام تحوي الكثير من المحتوى الذي يهدد السلام و السلم[4].

---

[1] - البهي ، الردع السيبراني ، مرجع سابق.

[2] -صباح عبد الصبور عبد الحي ،"استخدام القوة الالكترونية في التفاعلات الدولية الجزء الرابع"المعهد المصري للدراسات (2016)،آخر تحديث 19 نوفمبر2016

https://eipss-eg.org/ استخدام- القوة – الالكترونية –في –التفاعلات –الدولية –الجزء -الرابع/

[3] - ليلى الشهيل،" سيلفي عسكري"الجديد ،العدد الرابع (2015)
http://www.aljadeedmagazine.com/?id=546

[4] - مليكة كركود ،" الكتائب الالكترونية الدول تفقد سيادتها في حروب مواقع التواصل الاجتماعي "،France 24 (2016) ،آخر تحديث 11 أكتوبر2016

و في ظل هذه العولمة الإعلامية و الثقافية و المعلوماتية الفورية و المفتوحة والمترابطة بشكل لا سابق له تم تعبئة الشبكات الإجتماعية من طرف الدول بغرض مناصرة أجندة عسكرية معينة مستخدمة في هذا الصدد كل أساليب الدعاية و الاشاعة و الخداع حتى يصل الأمر لافتعال الأزمات بهدف اثارة القلق و ابراز التفوق المادي و التقني و حتى العسكري، كما تحول المحتوى للتقليل من قوة الخصم من التهديد و الوعيد إلى الاغراء و الاغواء و كافة سبل المناورات للاستفادة من التناقضات و الاختلافات المميزة لدى العدو كما يتم استعمال هذه الوسائط لترتيب المعلومات الأمنية و السياسية و حتى الشخصية عنه و كل ما يتعلق بالأمور العسكرية المصنفة في خانة السرية لخوض الحرب النفسية متخذة من مواقع التواصل الإجتماعي مسارحا لها فقد لعبت دورا هاما في تفعيل النشاط الارهابي مثلا بما وفرته و الترويج له من مصادر شديدة الأهمية للمتطرفين العارفين بالتكنولوجيا و يعد الموقع انستغرام الخيار الأمثل لدى كل الارهابيين المدعوين بالمجاهدين و المجموعات الجهادية الرسمية التي تستخدمه لتجنيد الأعضاء الجدد و حشد الأتباع.

وكما تستخدم الجماعات و المتمردون منصات الشبكات لمقاومة عنف الدولة وحتى التفاوض معها، يستعمل آلاف المواطنين عبر العالم مواقع الشبكات الإجتماعية [1]لاعلان مواقفهم المؤيدة أو المعارضة للسياسات المختلفة بل يستخدمونها كمصدر لمتابعة ما يجري بعد أن تحولت من آداة لمخاطبة العالم إلى وسيلة لفضح الممارسات العسكرية اللاخلاقية للجنود و الجيوش و هو ما استدعى اعادة النظر من طرف القيادات العسكرية في مسألة حمل الهواتف الذكية و الكاميرات من طرف الجنود أثناء تنفيذ العمليات العسكرية[2].

ونظرا للتأثير الطاغي الذي اكتسبه الفضاء الرقمي اثناء فترات الحروب ظهرت سياسات تستهدف التشكيك digital suspicion في المواد التي تسير بالوسائل الرقمية،والتي تنتهجها بالأخص الحكومات فبسبب حملات التضليل المتعمدة اصبح المتحدثون العسكريون الرسميون يدعمون تصريحاتهم بمقاطع حية محملة من الحرب ممّا خلق حملة أنتقادات واسعة و هكذا ذهب أنستغرام للحرب شأنه المدرعة الحربية رغم أن هذا الأمر لم يولد الا مزيدا من عدم اليقين بسبب التصريحات المضادة و يمكن القول أن وسائل التواصل الإجتماعي وشبكات الإتصالات ساهمت بشدة في صعود دور الفرد في الشؤون الدولية.

ثالثا:التجسس الألكتروني:

يعد التجسس أحد الأنواع و السبل الملتوية في الحروب القديمة و الحديثة اذ أنه يمثل " عملية الحصول على معلومات ليست متوفرة عند العامة "[3].

و يعد التجسس نوعا من أنواع الاختراق الذي " يقتصر على معرفة محتويات النظام المستهدف بشكل مستمر دون الحاق الضرر به "

كتائب-الالكترونية-مواقع-التواصل-الاجتماعي-الشارقة20161111/www .ar/com 24 france

[1] - أحمد الشورى ،" هل تشكل مواقع التواصل الاجتماعي تهديدا للأمن القومي"، السياسة الدولية(2015)،آخر تحديث 07 سبتمبر 2015 http://www.siyassa.org.eg/News/15182/

[2] - Adi Kuntsman and Rebecca L Stein, "Digital Melitarism Israel's occupation in the social media age ",

[3] - جاسوسية رقمية "، موسوعة ويكيبيديا ،(2018)آخر تحديث 31 ماي 2018

https://ar.wikipedia.org/wiki/ جاسوسية -رقمية /

وذلك عن طريق استخدام الانترنت و تحميل برامج خبيثة تسهل قدرة حكومة معينة على مراقبة حكومات أخرى عبر بعث الرسائل المزورة و انشاء الحسابات الزائفة على وسائل التواصل الإجتماعي أو البريد الالكتروني ،اذ يتم كشف هوية الضحية من الشركات المزورة لخدمات الانترنت و بمجرة نقر هذا الأخيرة على الرابط أو فتحه لبريد الكتروني يصبح عرضة لتسريب رسائله و انتهاك خصوصيته.

إن التجسس الرقمي او " التحكم في تغير القواعد بيانات الأشخاص قد تصل خطورته حد تهديد الأمن القومي لبعض الدول خاصة اذا ما علمنا أن " الأشخاص المستهدفين غالبا ما يكونون مسؤولين سامين أو علماء مرموقين[1].

والجدير بالذكر أن بعض المحاكم الدستورية العليا في الدول الكبرى تسمح باستخدام تقنيات التجسس على أجهزة الكمبيوتر و الهواتف الذكية مع وضع ضوابط مشددة على هذا الأمر ،ومن أمثلة هذا برنامج التجسس الألماني المسمى " حصان طروادة الاتحادي " و الذي يستعمل لدعم عمليات التحري والذي يقوم بفتح " الأبواب الخلفية " للأجهزة التي ينصب عليها و يمكن مرسليه حينئذ من معرفة كل مايقوم به صاحب الكمبيوتر و الهاتف المستهدف بداية من التنصت على المكالمات ونسخ الملفات حتى رؤية عدسة الكاميرا.

ويجب الاعتراف أن ما يتسرب عن الأساليب الحكومية للتجسس يعتبر قدرا ضئيلا جداً مقارنة بالمقدرات الخفية لها ، فالولايات المتحدة الأمريكية مثلا استطاعت التجسس على 30 دولة[2] بنجاح.

بعد أن توصلت لاخفاء برمجيات العمليات التجسسية في أعماق محركات الأقراص الصلبة التي تنتجها شركات كبرى مثل وستون ديجيتال وسيجيت و هو الأمر الذي وفر للوكالة امكانية التجسس على أغلبية أجهزة الكمبيوتر في العالم.

وقد طورت الولايات المتحدة هذه التقنية حتى أصبح التجسس الالكتروني يعرف " بحرب التجسس المعلوماتي " و التي تمثل " عدة طرق لاختراق المواقع الالكترونية و من ثم سرقة بعض المعلومات وقد انتشرت بقوة في العقدين الأخيرين وشمل الاختراق المؤسسات العسكرية و التقنية خاصة البنوك المركزية و المؤسسات العملاقة، في حين تعني الجاسوسية الرقمية " التسلل إلى الأجهزة الحاسوبية و محاولة اعتراض الاشارات وحزم المعلومات المرسلة عبر الانترنت.

ويتم استغلال الثغرات الأمنية أو إختراق أمن الحاسوب security cracking في الحواسيب الموصلة بشبكة الحاسوب للحصول على المعلومات المخزنة في الكمبيوتر، و قد أعطت

---

[1] -"جاسوسية رقمية "،مرجع سابق

[2] - يوسف ت، "أشهر عمليات التجسس الرقمية في الخمس سنوات الأخيرة" ، ،طلائع الجزائريين ،مكتب الدراسات الاستراتيجية الأمنية ،المرصد الجزائري(2017)، آخر تحديث 27 مارس 2017
http://marsadz.com/

الحكومات أهمية خاصة للتجسس الالكتروني و حل حد تطوير برامج خاصة بالتجسس أشهرها على لإطلاق برنامج كارنيفور و شبكة إيشلون.

من أشهر برامج التجسس الإلكتروني نعد:

أ- برنامج كارنيفور "carnivor" أو ملتهم البيانات:

كارنيفور برنامج صمم من قبل وكالة المباحث الفيدرالية الأمريكية[1]بالتعاون مع الشركة المزودة لخدمة الأنترنت "يسمح بجمع معلومات محددة حول رسائل البريد الالكتروني أو أية اتصالات إلكترونية واردة أو صادرة من المستخدمين المستهدفين بتحقيق ما " وقد جاء اعتماد هذا النظام الكمبيوتري تطبيقا لأمر محكمة أمريكية ، وتعني كلمة كارنيفور بالانجليزية آكل اللحوم أي أنه برنامج مصمم " لمضغ "[2] كافة البيانات المتدفقة عبر أي شبكة اتصالات، ويستخدم " المتلهم " بشكلين فقط:

الأول رصد المعلومات الواردة و الصادرة من حساب بريدي الكتروني معين ورصد حركة البينات دون المحتويات الفعلية.

و الثانية هي رصد جميع الأجهزة المزودة (مزودات الويب و الملفات) التي يقوم المستخدم بالنفاذ اليها دون رصد المحتوى الفعلي لما ينفذ اليه المستخدم.

كما يمكنه رصد جميع المستخدمين الذين ينفذون إلى صفحة ويب معينة أو رصد جميع صفحات الأنترنت و ملفات FTP التي يقوم المستخدم بالنفاذ اليها.

و يتم ذلك بعدة طرق منها رصد جميع الترويسات headers الخاصة برسائل البريد الالكتروني.

ب- **شبكة ايشلون Echelon** :

هو نظام عالمي لرصد بيانات و اعتراضها و نقلها ثم تشغيلها من قبل المؤسسات الاستخباراتية لخمسة دول هي الولايات المتحدة الأمريكية و المملكة المتحدة وكندا و استراليا و نيوزيلندا[3].

و يعتقد أن ايشلون هي كلمة انجليزية الأصل تختص التسمية بجزء من النظام الذي يقوم باعتراض الإتصالات التي تتم عبر الأقمار الصناعية ،فاستناداً لاتفاقية UKUSA التي وقعت سنة 1947 تقوم المؤسسات الاستخباراتية لتلك الدول بالتنسيق فيما بينها، و رغم أن نظام ايشلون المستخدم حاليا لم يبدأ العمل الا سنة 1971 الا أن نطاقاته و قدراته توسعت كثيرا حتى صارت

---

[1] - Michel Ktitareff ,"Le FBI utilise en secret un logiciel espion contre le cyberterrorisme", Les Echos .fr(2001),27 novombre2001
https://www.lesechos.fr/27/11/2001/LesEchos/18539-058-ECH_le-fbi-utilise-en-secret-un-logiciel-espion-contre-le-cyberterrorisme.htm

[2] -"جاسوسية رقمية "،مرجع سابق

[3]/ -"ايشلون .،..أذن الشيطان ..أو كيف تتجسس أمريكا على العالم"،منتدى الجيش العربي(2013)آخر تحديث28 أكتوبر 2013
http://www.arab-army.com/t84615-topic

تشغل كافة أرجاء المعمورة بعد أن استطاع ايشلون اعتراض و تعقب الكثير من ثلاثين مليون عملية اتصال يوميا بدءا من المكالمات الهاتفية العادية حتى اتصالات الانترنت.

وتتم عملية جمع الإتصالات و من ثم تصفيتها و غربلتها باستعمال برامج الذكاء الاصطناعي بغرض انشاء التقارير الاستخباراتية حتى أنه هناك اعتقاد أن شبكة ايشلون تتجسس على 90% من المعلومات المتداولة عبر الانترنت[1].

ج- أنفوبول Enfopol

و نظرا لأهمية التجسس الرقمي في جميع البيانات و المعلومات المطلوبة من أجل ضمان الأمن القومي للدول فقد صدر عن الاتحاد الأوروبي وثيقة أطلق عليها " **أنفوبول Enfopol**"، تحوي كافة المتطلبات التقنية التي تقوم بتسهيل عملية التنصت للجهات الأمنية عبر أوروبا و يجري حاليا تطبيق هذه المقاييس على نظم الإتصالات في جميع أرجاء أوروبا.

د- الو م أ calea:

يفرض القانون الأمريكي[2] على جميع الشركات المزودة لخدمات القيام بتعديل معداتها وقدراتها حتى يتسنى للجهات الحكومية استخدامها لأغراض التنصت و التجسس.

رغم الاجراءات الحكومية التي تتضمن الاعتراف بعمليات التجسس عبر السماح بتقنين خدماته الا أنه يظل عملية غير مشروعة اضافة إلى أنه يمثل " تربصا و خطرا داهما".

فالتجسس الالكتروني هو شكل آخر من أشكال الارهاب يقوم باستخدام التكنولوجيا بشكل ضار و يؤدي لاحداث آثار مدمرة و أضرار بالغة و كبيرة لمحطات التحكم وشبكات الاتصال كما يهدد العلاقات السياسية والدبلوماسية الدولية حتى أنه يعرف بـ " العدوان و التخويف أو التهديد " المادي و المعنوي الصادر عن الدول و الجماعات و الأفراد على الانسان بغير وجه حق.

حيث باتت الشبكة قادرة على التقاط 100 مليون اتصال شهريا وضعت كلها لخدمة أهداف تجسسية صناعية و اقتصادية و تكنولوجية. ، أقيمت قواعد عسكرية لها في كل من منطقتي " موروتينوس " و " مين ويزهيل" ويرمز لها بالمحطة " إ ف 38 " تتم فيها عملية المراقبة باسم قانون "ستيل بوش "[3]

و تجدر الاشارة إلى أن القانون الدولي الذي يدين قرصنة الإتصالات الهاتفية لم يتعرض للاتصالات عبر الأقمار الصناعية وهو الأمر الذي صعب على الدول الممتعضة من نشاطات شبكة ايشلون وضع حد لها خاصة و أن عملياتها الاستخباراتية منحت الفرصة للشركة الأمريكية

---

[1]- "Le système Echelon :une nouvelle donne dans l'espionnage électronique »,institut québécois des hautes études internationales, (université LAYAL,bullettin N° 50 janvier 2001)
http://www.cms.fss.ulaval.ca/recherche/upload/hei/fichiers/bulletin50.pdf

[2] -"جاسوسية رقمية "،مرجع سابق.

[3]- "حرب الانترنت" ،موسوعة ويكيبيديا الحرة (2018) ،آخر تحديث 08 جانفي 2018
https://ar.wikipedia.org/wiki/حرب_الانترنت

الشهيرة ماكدونالد دوغلاس مثلا احتكار صناعات معينة بما توفر لديها من معلومات من "إيشلون".

كما ألحقت استخباراتها خسائر قدرت بــ 30 مليون فرنك فرنسي ، اذ خسرت شركة تومسون الفرنسية مثلا 2 مليون دولار بسبب الشروط المالية الصعبة التي و ضعتها أمامها الولايات المتحدة لصالح صناعات رادارات أمريكية من طراز " رايثون "و هو الدليل على أن شبكات التجسس غدت أكثر أهمية من سلطات الدول و باتت تهدد بصمت الأمن و الاستقرار العالميين بعد تفجيرها للأزمات بين الأطراف الدولية في ظل صعوبة مراقبتها و الحد من نشاطاتها.

و قد استدعى التصدي للشبكة احداث عمليات تعديل و اسعة النطاق على الأجهزة الالكترونية التابعة لمعظم القطاعات في الدول الأوربية خاصة.

وتتمثل خطورة التجسس الالكتروني أنه لا يترك أي دليل مادي مما يصعب عملية التحقيق و اكتشاف الفعل التجسسي بسبب سهولة اتلاف الأدلة حال العثور عليها. ورغم اعتماد أغلب حكومات العالم على آليات التجسس بغرض التقصي و الاستقصاء الا أن عقوبة التجسس لا تزال و خيمة تصل إلى حد الاعدام بما أن الدول تقارن و قائع التجسس الالكتروني و التدخل في الشؤون الداخلية بالارهاب كما وصفه المتحدث الرسمي باسم الكرملين ديميتري بيسكوف رفقة زعماء البريكس[1].

المطلب الثاني:أشكال العسكرة الرقمية

أولا: الحرب السيبرانية.

1- تعريف الحرب السيبرانية

يشير مصطلح الحرب السيبرانية إلى استخدام الحواسيب و شبكة الانترنت في مهاجمة الأعداء ويدعى هؤلاء بالمخترقين أو الهاكرز hackers[2] وقد كانت أولى محاولات إطلاق الحروب السيبرانية سنة 1993 بعدما شاع تعبير "ضربات من غير هجوم" hitting without holding[3] و الذي شكل النقلة النوعية التي أحدثتها ظهور الحروب السيبرانية على الساحة الأمنية والدولية حولت المفاهيم وقلبت الموازين، فإحداث أكبر قدر من الخسائر البشرية والمادية لم تعد الغاية المباشرة المتوقعة من الحروب.

وفي مقال بعنوان " الحرب السيبرانية قادمة " قدم الكاتبان John Arquilla and David

Ronfeldt تعريفا للحرب السيبرانيةعلى أنها "اجراء و الاستعداد لاجراء العمليات العسكرية بالاعتماد على المبادئ و الآليات المعلوماتية ما يعني تعطيل ان لم يكن تدمير نظم المعلومات و الاتصالات على أوسع نطاق لتشمل حتى العقيدة العسكرية للعدو و التي يعتمد عليها لتحديد أهدافه و

---

[1]-"جاسوسية رقمية "،مرجع سابق

[2]- "حرب الانترنت" ،موسوعة ويكيبيديا الحرة (2018) ،آخر تحديث 08 جانفي 2018
https://ar.wikipedia.org/wiki/حرب الانترنت

[3]-سارة عبد العزيز،" الحرب السيبرانية"، مرجع سابق.

التحديات التي يواجهها "[1] معبرين بذلك عن النمط الأول من أنماط الحروب السيبرانية التي يتم فيها توظيف القوة الصلبة في الصراع الرقمي.

كما تطرقا للمفهوم الثاني و الذي يمثل نمط آخر من الحروب الرقمية والذي يوظف القوة الناعمة في الصراع وهو حرب الشبكات netwar التي تعني "شن الصراعات الفكرية على المستوى المجتمعي من خلال الانترنت "الأمر الذي يحدد كيف لثورة المعلومات أن تغير من كيفية دخول المجتمعات دائرة الصراع العسكري و الفكري، و رغم تعدد التعاريف و عدم وجود تعريف واحد متفق عليه لمفهوم الحرب الرقمية فان الاختلاف الوحيد يكمن في اقتصار الفاعلين على الدول دون غيرها حتى يمكن تمييزها عن الارهاب أو في تقدير حجم الخسائر والتداعيات المترتبة عن تلك الحروب فمصطلح الحرب الرقمية يستخدم للتعبير عن حالة توجه جديد يعمل لتوظيف الأنشطة العدائية التي يزدحم بها الانترنت بما يميزها عن الجريمة الرقمية و الارهاب الرقمي.

وفي الوقت الذي ينطوي فيه الاختلاف الأول على ضرورة تضمن الفاعلين من غير الدول في تعريف تلك الحرب سواء بشكل منفرد أو بالنيابة عن الدول والتي تمثل وجهة النظر الروسية خاصة، تذهب بعض وجهات النظر إلى اقتصار مفهوم الحرب الرقمية على ما تضمنه تعريف قدمته دراسة صادرة عام 2015 عن " مركز ابحاث الكونغرس "[2] في الولايات المتحدة الأمريكية أن الحرب السيبرانية تمثل " إجراء من دولة ضد أخرى بما يعادل الهجوم المسلح أو استخدم القوة في الفضاء السيبراني و الذي قد يؤدي إلى رد فعل عكسي باستخدام القوة التقليدية المناسبة".

أما الاختلاف الثاني فيتمثل في حصر بعض التعريفات لممارسة النشاط العدائي على الأجهزة الاعلامية وشبكات التواصل الإجتماعي فيما تضيف التوجيهات الأخرى الأنشطة الدفاعية و الهجومية السيبرانية التي تشكل خطر على البنية التحتية و النظم العسكرية، غير أن كل هذه التعويضات تتفق على تجاوز المفهوم التقليدي للحرب الذي يرتكز أساسا على إستخدام الجيوش النظامية و المسبوق بإعلان واضح لحالة مع وجود ميدان قتال محدد إلى عدم محدودية المجال و الأهداف تنقسم الحرب الرقمية إلى شقين: شق دفاعي و آخر هجومي و يتمثل الشق الأول في سبل الحماية الالكترونية و التي مهمتها حماية مكونات الفضاء الرقمي المادية و المعنوية و أدواته و اجراءات عمله وكذا الأفراد القائمين عليه.

أما الشق الهجومي فيتميز بعنصر المباغتة الذي تكون له الغلبة بغض النظر عن حجم قدراته العسكرية التقليدية.[3]

ثانيا: أنماط الحروب السيبرانية:

1- **النمط الأول: الحرب السيبرانية منخفضة الشدة[1] :** أو ما يسمى بالحرب الرقمية الباردة التي تتخذ الحرب النفسية و الاختراقات المتكررة و التجسس و سرقة المعلومات فضلا عن حروب الأفكار

---

[1]- مرجع سابق.

[2]- سارة عبد العزيز، "الحرب السيبرانية"، مرجع سابق.

[3]- Michel Hermans, " La guerre numérique"
Michel.Hermans@ulg.ac.be " ,
https://orbi.uliege.be/bitstream/2268/168643/1/La%20guerre%20num%C3%A9rique.pdf

وحمى التنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية. ويتجلى هذا النمط خاصة في الصراعات السياسية ذات البعد الإجتماعي والدين الممتد كالصراع العربي- الاسرائيلي و الصراع الهندي-الباكستاني أو الصراع القائم بين الكوريتين الشمالية والجنوبية.كما تتميز حروبه بأنها تتسبب في نشوء أزمات دولية مثل التوتر بين طهران وواشنطن، كما تعد هجمات إيران الرقمية على المنشآت النفطية السعودية والتي استعملت فيها فيروسات متنوعة كـ " دوكو " سنة 2012، وفيروس شمعون سنة.2017 . كمايمكن إدراج هجمات روسيا على النرويج و المملكة المتحدة في اطار الحرب المنخفضة الشدة.

2-النمط الثاني: الحرب الرقمية متوسطة الشدة: هي التي تتم تمهيداً لعمل عسكري مباشر أو بالموازة مع الحرب التقليدية الدائرة على الأرض معبرة عن حدة الصراع القائم وتعمد فيه الأطراف لتخريب المواقع الالكترونية وتدميرها وتعزى شدة الصراع لارتباطها بالعسكرة التقليدية خاصة و أنها لا تكلف سوى ربع نفقات نظيرتها التقليدية أي " يتم تمويل حملة حربية كاملة عبر الانترنت بتكلفة " دبابة" [2] وقد ظهرت الحروب المتوسطة الشدة في هجمات حلف الناتو عام 1999 على يوغوسلافيا حيث استهدفت شبكات الإتصالات للخصوم و تسببت بتعطيلها كما برزت خلال الحرب بين حزب الله و اسرائيل عامي 2008 و 2012 وكذلك في حرب روسيا وجورجيا عام 2008.

النمط الثالث: الحرب الرقمية مرتفعة الشدة : و الحرب الرقمية الساخنة و تتميز بشن حروب رقمية منفردة و غير متوازية أو مرتبطة بالأعمال العسكرية التقليدية ورغم عدم حدوثها على أرض الواقع الا أن توقعات نشوبها كبيرة خاصة مع تطور القدرات التكنولوجية و بروز الحكومات الالكترونية.

وتتم ادارة الحرب عن بعد وذلك بتوجيه الآليات "الروبوتات" و الطائرات من دون طيار مع الاستحواذ التام على القوة الرقمية سواء كان ذلك في مجال الدفاع أو الهجوم وتقوم الدول باستهداف الحياة المدنية و البنية التحتية المعلوماتية بهدف " الهيمنة الالكترونية الواسعة "، و ما يسمى يرجح احتمالات حدوث هذا النمط هو التطور السريع للأسلحة الالكترونية خاصة بعد استعمال الفيروس الخطير ستوكنت من طرف قوى دولية كبرى [3].

و يصعب التحكم في مصير الحروب الرقمية بحكم اتخاذها للفضاء السيبراني المتقلب كمسرح حرب وباعتبار تحركاتها عبر شبكات المعلومات و الإتصالات متخطية بذلك الحدود الدولية و معتمدة على أسلحة إلكترونية متجددة تلائم السياق التكنولوجي لعصر المعلومات.

ثالثا: خصائص الحرب الرقمية

تتميز الحروب السيبرانية بجملة من الخصائص أهمها:

- عدم معلومية مصدرها.

---

[1]- عادل عبد الصادق، "الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي" المركز العربي لأبحاث الفضاء الالكتروني (2018)،آخر تحديث 11 مارس2018
http://accronline.com/article_detail.aspx?id=29088

[2]- عبد الصادق ،"الهجمات السيبرانية"،مرجع سابق.

[3] -عبد الصادق ،"أنماط الحروب السيبرانية"،مرجع سابق.

- عدم امكانية معرفة الحجم الفعلي للخسائر.[1]
- جهل الكيفية التي تم بها الهجوم.

وتدخل هذه الحروب في اطار الحروب غير المتكافئة: كون الحرب لا تناظرية asymmetric[2] أي أن الطرف الذي يبادر باستخدام القوة الهجومية يعتبر الطرف الأقوى بغض النظر عن حجم قدراته العسكرية مما يؤثر على نظريات الردع الاستراتيجي ويجعلها غير فعالة البتة.

-انخفاض التكاليف: اذ لا تحتاج الحروب الرقمية لأعداد كبيرة من القوات و الأسلحة كما تنخفض تكاليف دخول المجال السيبراني الا فيما يخص تكاليف عمليات التطوير وبناء الكفاءات اذ بدأت الدول في اعداد ميزانيات خاصة لاستثمار واسع في هذا المجال[3].

-سهولة الاختراق بسبب التطور التكنولوجي السريع: فأنه حتى باعتماد الأنظمة الدفاعية الدقيقة يظل هامش الخطر كبيرا دوما.

-الطبيعة غير المتماثلة للحروب السيبرانية: فغالبا ما يعد الهجوم تفوقا للمهاجم على الهدف أو قصورمسجلا من قبل الدفاع لدى الطرف المستهدف.

-حروب الانترنت حروب لا تناظرية [4](asymmetric)

-انتفاء أدلة الادانة: ذلك أن الهجمات السيبرانية غالب ما تأخذا طابعا سريا مما يفتح المجال لتخمينات واسعة تتم عبرها محاولة ربط الأحداث بعضها ببعض دون توفر أدلة قاطعة تدين جهة محددة[5].

ونهاية ، يمكن القول أن أهم ما تختص به الحروب السيبرانية هو احداثها لنطاق واسع من التداعيات والذي يرجع بالأساس للترابط الكبير بين شبكات القطاعات الحيوية بالدولة، اذ يمكن لهجمة رقمية واحدة تعطيل وتدمير شبكات كاملة مع ما يرتبط بها من بنية تحتية على أوسع نطاق ممكن أي أن آثارها تتجاوز بكثرة قدرة الأسلحة التقليدية في خلق الأضرار مع تسجيل فعالية كبيرة ودقة قصوى في تحديد الأهداف وهي الخاصة التي تؤكد سابقتها، فستطاعة الهجمات الرقمية تحديد الهدف المراد مهاجمته بدقة متناهية و إصابة في لحظات دون حتى تفطن الضحية لذلك[6] وهو الأمر الذي شجع الفواعل المختلفة للانخراط في استخدام السلاح الرقمي كبديل للسلاح التقليدي

[1]-Ibid,Richard A Clarck," cyberwar,"37

[2]- علي حسين باكير ،" المجال الخامس ... الحروب الالكترونية في القرن ال21"،مركز الجزيرة للدراسات(2011)،آخر تحديث 12 جانفي2011 http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

[3] Ibid , Richard A. Clarke and Robert K. Knake ,"cyber war" , 38

[4] - عبد الصادق،"خطر الحروب السيبرانية عبر الفضاء الالكتروني"،(2017)آخر تحديث سبتمبر 2017
http://aitmag.ahram.org.eg/News/83562.aspx

-1 عبد الصادق ،" الهجمات السيبرانية "،مرجع سابق

[6] Ibid,"cyberguerre : concept, état d'avencement »

كوسيلة بديلة لتصفية الحسابات وترجم هذا الأمر فيتعاظم الحرب الرقمية لتشكل البعد الرابع بين أسلحة القتال .[1]

خاصة مع عدم وجود مظلة قانونية اذ أنه رغم الجهود المبذولة لتنظيم العمليات التي تجري في ساحة الحرب الرقمية من قبل القانون الدولي لا توجد لحد الآن قواعد ولو حتى مبدئية و قوانين تعمل على الحد من الافراط في استخدام القوة الرقمية.

المبحث الرابع:المقاربات النظرية للعسكرة الرقمية

لقد شكلت العسكرة الرقمية لوقت طويل مفهوما واضحا لطالما اعتمدت عليه النظريات الكبرى في العلاقات الدولية لما احتوته من دلالة وحيدة مرادفة للقوة المادية و التي ترتكز أساسا على امتلاك و تطوير السلاح التقليدي أساسا غير أن ظهور العسكرة الرقمية وسع من دائرة النطاق المصطنع الذي تشابكت فيه فقد أدى الاعتماد على الآليات التكنولوجية الحديثة في ادارة التفاعلات الدولية إلى إحداث تغييرات واسعة في مفاهيم القوة و الأمن و الصراع و التي لطالما شكلت محورا رئيسيا للجدال بين المنظورات الرئيسية للعلاقات الدولية بشكل أصبح فيه الفضاء الالكتروني يشكل تحديا كبيرا خاصة فيما يتعلق بخاصيتي تعدد فواعله و تصاعد دور القوة النسبية من خلاله.

المطلب الأول : الواقعية [2]

لقد كان لظهور العسكرة الرقمية كبير الأثر في دحض حجج و قواعد كبريات المدارس النظرية في العلاقات الدولية فرغم أن افتراضات المدرسة الواقعية لم تتغير في الأساس بعد نهاية الحرب الباردة كونها تصر على الدولة كفاعل وحيد مسيطر في المجتمع الدولي كما تعطي الأولوية للبعد العسكري للقوة خاصة مع غلبة الطابع الصراعي على العلاقات بين الدول[3] مما يعني أن الدولة تستقي عناصر قوتها من المكونات المادية كتعداد السكان و معدل الانفاق العسكري، الا أنها تطورت تماشيا مع المتغيرات الجديدة، إذ ميزت أولا بين امتلاك عناصر القوة و القدرة على استخدامها، بما أن مجرد *امتلاك* عناصر القوة للدولة لا يعني بالضرورة القدرة على التأثير في الآخرين، و هو الاتجاه الذي يعبر عن القوة كمسافة أين يكون إمتلاك القدرات يعتمد بشكل كبير على متغيرات وسيطة يمكن ترجمتها بحيازة النفوذ و التأثير الخارجي، و قد أخذ هذا المفهوم في

---

[1] سامر مؤيد عبد اللطيف ،"الحرب في الفضاء الرقمي رؤية مستقبلية "، مركز الدراسات القانونية و الدستورية،مجلة رسالة الحقوق ، جامعة كربلاء ، السنة السابعة، العدد الثاني (2015)
https://www.iasj.net/iasj?func=fulltext&aId=104012

[2] **-" ترتكز النظرية الواقعية على جملة من المبادئ الرئيسية التي يصر عليها رواد المذهب الواقعي ك:اعتبار الدولة الفاعل الأساسي في العلاقات الدولية و بالتالي اعتمادها وكحدة تحليل أساسية .**

-ضرورة اعتماد الدولة على قوتها الذاتية و العمل على زيادة القوة العسكرية التي تضمن لها التفوق و الريادة في المجتمع الدولي.

-تأثير الموقع الجغرافي للدولة على امكانياتها و توجهاتها السياسية.

-عدم صلاحية اعتماد الرأي العام كمرشد لصانع القرار من حيث طبيعته المتغيرة"

- مي حسين عبد المنصف ،"النظرية الواقعية الكلاسيكية في العلاقات الدولية" ،الحوار المتمدن،العدد 4068 (2013)،آخر تحديث 20 أفريل 2013
http://www.ahewar.org/debat/show.art.asp?aid=35533

[3] - محمد فرج أنور ،"نظرية الواقعية في العلاقات الدولية "،مركز كردستان للدراسات الاستراتيجية (2007)،318 ،آخر تحديث

التوسع إذ ظهرت من رحم المدرسة التقليدية ما أطلق عليه بالواقعية الجديدة [1]و التي اعتمدت بالأساس على المنهجية الاقتصادية و غيرها من الاتجاهات النظرية التي اهتمت بتطويع فروض النظريات الأساسية في العلاقات الدولية و التي أخذت على عاتقها بالأساس تفسير سلوك الفاعلين من غير الدول، بافتراض أن سلوك هذه الأخيرة مشابه لسلوك الدولة اذ تجاهد الفروض الواقعية بأن تأثير الفواعل غير الدولاتية يتم من خلال الدولة و الدولة وحدها و التي تحتل مكانة مهمة في الفكر الواقعي[2] ، و قد قامت هذه الاتجاهات بتطوير أطر من الفاعلين غير الدوليين عبرنماذج عامة استندت إلى معايير شتى رغم أن أبرزها استنادا تمثل في انخراط الفاعل في تفاعلات عابرة للحدود[3]. كما أكدت على ظهور أدوات بديلة عن القوة العسكرية ،و هي الطروحات التي لم تشكل العسكرة الرقمية تحديا لها فحسب بل أكدت على بطلان الكثير من مبادئها فظهور الفضاء الالكتروني و التهافت الذي سجل من طرف الفواعل الدولية المختلفة، دول، منظمات، مجموعات و أفراد لاتخاذه كساحة صراع حديثة، ضرب كل محاولات تجديد النظرية الواقعية في الصميم فلا الدولة استطاعت الصمود كفاعل رئيسي في العلاقات الدولية و لا الاعتماد على القوة الصلبة غدا وسيلة يعتمد عليها لتحقيق الأمن القومي الوطني، فلطالما تطلب محاولة فهم و تحليل الصراعات الدولية بغية إعطاء صورة واضحة للتفاعلات الدولية تحديد دقيق لمعنى و مفهوم القوة و التي تعد أحد المفاهيم المحورية في العلاقات الدولية.

فالقوة و التي عنت حيث الفيلسوف الصيني "سان زو" " القدرة على شن الحروب. حيث أن العمليات العسكرية مهمة للأمم و الشعوب و هي أساس الحياة أو الموت" و التي ساد مفهومها حتى عصر مكيافيلي الذي رأى أن القوة " تشكل عنصرا من العناصر الأساسية لقيام الدولة بما أن وجود هذه الأخيرة يعتمد عليها بالدرجة الأولى".[4]

و لطالما ظلت القوة الصلبة كنمط تقليدي للقوة التي عرفت منذ الأزل تستخدم للسيطرة على القوة المادية بما أن الدول تستخدم وسائل مختلفة لتحقيق أهدافها مترجمة قدراتها بواسطة " الدبلوماسية و القوة العسكرية و الدعاية و الأدوات الأقتصادية" الا أن مصادر و أشكال القوة تغيرت بمرور الزمن إذ تزايد الاهتمام بالأبعاد غير المادية للقوة بعد انتشار الثورة المعلوماتية والتقنية، حيث لم يعد امتلاك الدولة للثروات و الأموال و الأسلحة الثقيلة كافيا لبلورة دورها كقوة فاعلة و مؤثرة في النظام الدولي بعد أن انخفضت الحواجز في عصرنا الحالي "عصر الثورة الصناعية الثالثة"[5] التي منحت للفواعل الجدد خاصة الأفراد منهم الفرصة ليلعبوا دورا مباشرا في السياسة العالمية و هو الأمر الذي أتاحه هبوط تكاليف الحوسبة و التطور السريع في الإتصالات و البرمجيات مما سمح بتوزيع القوة على نطاق واسع، و هكذا استطاعت كل هذه الشبكات غير

---

[1] -عزت عبد الواحد ،"مقومات وسياسات الأمن القومي" ،المنهل (2017)،أطلع عليه بتاريخ 08 ماي2 018https://platform.almanhal.com/Files/2/84256

[2] - عبد الوهاب جعيجع ،"الأمن المعلوماتي و ادارة العلاقات الدولية "،الموسوعة الجزائرية للدراسات السياسية و الاستراتيجية (الجزائر :دار الخلدونية، الطبعة الأولى ،2016) آخر تحديث01 جانفي 2018

https://www.politics-dz.com/community/threads/almn-almylumati-u-dar-alylaqat-alduli.10851/

[5] -فريدة طاجين ،"دور مجتمع المعلومات في تعزيز الأمن الانساني : دراسة حالة ماليزيا " (أطروحة مقدمة لنيل شهادة دوكنوراه العلوم في العلوم السياسية و العلاقات الدولية ، تخصص علاقات دولية ،جامعة بسكرة ،2015 2016) ،26

الرسمية العمل على تقليص احتكار البيروقراطية التقليدية للقوة فتغيرت بذلك مصادر تهديد الأمن القومي الوطني بعد أن أضحت مجابهة الأخطار بالقوة التدميرية للأسلحة التقليدية غير ذات فائدة بسبب تحول تكنولوجيا الإتصالات لمصدر جديد للتهديد طال العام و الخاص خاصة و أنها أقل كلفة و أسرع وتيرة مقارنة بنظيرتها التقليدية و التي صار إستعمالها مرفوضا جملة و تفصيلا لدى الرأي العام العالمي.

لقد شكل ظهور الأفراد كفاعلين عابرين للحدود القومية و تراجع القوة الصلبة بظهور القوة الناعمة كمحدد من محددات القوة التي اتخذت آداة للسياسة الخارجية بعد الحرب العالمية الثانية والتي استمر مفهومها بالتصاعد حتى تبلورت بمفهومها الواضح بعد نهاية الحرب الباردة دفعا كبيرا للعسكرة الرقمية[1] التي تترسخ يوما بعد يوم كنهج جديد تتبناه فواعل العلاقات الدولية كنهج للصراع الدولي.

المطلب الثاني : الليبرالية [2]:

طرحت القوة الناعمة كمصطلح عام 1995 من طرف المفكر جوزيف ناي سنة 1995 والذي ساهم تقديمها كرديف للقوة الصلبة في انتعاش أفكار المدرسة الليبرالية خاصة المؤسسية منها حيث رفضت هذه الأخيرة افتراضات الواقعية مبررة موقفها بتنامي أدوار الفاعلين الجدد و هو الدور الذي لا ينبغي تجاهله بأي شكل من الأشكال لما له من تأثير على سلوك الدول.

إن تصورات الليبرالية المنطلقة من أن الإنسان يعيش في إطار شبكات اجتماعية تساعده في تحقيق مطالبه مما يستوجب التناغم بين الفاعلين نتيجة الإعتماد المتبادل[3]، جعلت الإتجاه الليبرالي المؤسساتي يقدم تفسيرا أفضل لزيادة فاعلية توسيع المؤسسات الدولية كآلية للتحكم والتأثير في سلوك الدول حيث تستند هذه المؤسسات على نظام يتكون من مجموعة من المبادئ principes و معايير السلوك norms و قواعد rules و إجراءات تسمح بالتحكم في سلوك الفاعلين[4]في مجال

---

[1] - Ludwig Von Mises,"les fendement du libéralisme" , Le québécois libre, vu le 03mai2018

http://www.quebecoislibre.org/08/080120-2.htm

[2]-" تقوم الليبيرالية على مرتكزات تؤكد على :

أولا :الديموقراطية كنهج يحقق السلام و الأمن فهي تمثل تيارا سياسيا و ايديولوجيا يعبر عن مطالب الحريات الديموقراطية

ثانيا: الحرية الفردية و المساواة و التي تتحقق بعدم تدخل الدولة ،اذ يتفق الليبيراليون مع اختلاف توجهاتهم السياسية على أن الليبيرالية هي حرية المبدأ و المنتهى والباعث و الهدف و الأصل كذلك

ثالثا:التعاون بين مختلف الوحدات الدولية التي تتفاعل في تناغم وانسجام لتحقيق مصالحها الوطنية . "

[3] --أنور ،"نظرية الواقعية "،مرجع سابق

2- نصر الدين أوشن ،"النظرية الليبيرالية في العلاقات الدولية"(الجزائر : أم البواقي،جامعة العربي بن مهيدي،2012 2013) 1- -1

العلاقات الدولية[1] وقد شكل ظهور القوة الناعمة التي تعتمد على جاذبية " النموذج والاقناع" بدل القهر والقسر، وعلى الترغيب والجذب بدل الإكراه و الإجبار دفعة قوية لهذا الاتجاه فقد استعملت القوة الناعمة و التي تعرف بـ" cooperative power "[2] بأنماط متعددة منها السلبية والايجابية بين أطراف غير متماثلة في القوة فهي تعني "قدرة الدولة على خلق و ضع يفرض على الدول الأخرى أن تحدد تفضيلاتها و مصالحها بشكل يتفق مع هذا الاطار الذي يتم وضعه" فهي تمثل القدرة التي تؤدي إلى إحداث تغيرات سلوكية في أفعال الآخرين[3].

غير أن هذا الطرح يشوبه النقص ففي حين يمكن الاعتماد على الدور الذي تلعبه المؤسسات الدولية في تحديد سلوك الدول فإن ذات المؤسسات تقف عاجزة عن تحديد سلوك الفرد الذي غدا فاعلا رئيسيا و مباشرا في العسكرة الرقمية، بل و على العكس من ذلك سمح دوره المتنامي في منح فرصة للدول للتنصل من مسؤولياتها الجنائية وهو ما يتجلى في قيام الدول بتجنيد أفراد وجماعات للقيام بعمليات عدانية دون الاعتراف بها. كما أنه ينبغي الإعتراف[4] بأن القوة الناعمة لا يمكن أن تؤدي دورها المرجو دون وجود القوة الصلبة ومقدراتها التي تضمن لها القدرة على إحداث التغيير المطلوب، وهو ما يسمح بوجود القوة الصلبة كقيمة مضافة[5] أين ينتج لنا المزيج بين كلا المفهومين مفهوما جديدا، وهو ما يطلق عليه بالقوة الذكية وهو المصطلح الذي يعني تحديدا قدرة الفاعلين الدوليين على الجمع بين عناصر القوة الصلبة و القوة الناعمة بطريقة تضمن التحقيق الفعال و الكفؤ للأهداف المسطرة" مما يقتضي الفهم الذاتي و الإدراك الكلي للسياق الإقليمي الدولي الذي يتم في نطاقه تحقيق هذه الأهداف فالثورة التكنولوجية تمخضت عن ثورة أخرى هي الثورة في الشؤون العسكرية و إلتي اعتمدت على التفوق في المجال الرقمي كعنصر حيوي لتقديم عمليات ذات فاعلية في البحر و الأرض و الجو و الفضاء بعد أن غدت القدرة القتالية في الفضاء الالكتروني تعتمد على نظم السيطرة التكنولوجية.

إن ظهور الفضاء الرقمي كمتغير في العلاقات الدولية شكل تحديا صريحا واضحا للدور الذي لعبت عسكرته في تعظيم القوة أو الإستحواذ على عناصرها الأساسية في العلاقات الدولية، مما فسح مجالا جديدا أين تُمارس الفواعل المختلفة القوة الصلبة والناعمة على حد سواء ، وذلك بالتوجه نحو استعمال القوة الافتراضية، والتي تعني " القدرة على استخدام الفضاء الرقمي والمعلومات للتأثير في الأحداث على النحو الذي يحقق الأهداف المرجوة باستخدام الأدوات والوسائل الرقمية".

2- edu.academia.www/ 5510763 /

[1] - سعاد محمود أبو ليلة،"دور القوة :ديناميكيات الانتقال من الصلبة الى الناعمة الى الافتراضية "،السياسة الدولية (2012)،آخر تحديث 14 أفريل 2012
http://www.siyassa.org.eg/News/2376.aspx

[2] - غسان طه ،"الحرب الناعمة :القوة الجاذبة وأساليب المواجهة "، مركز الحرب الناعمة للدراسات (2015)،آخر تحديث 09 جويلية 2015
http://softwar-lb.org/4338/296/(الحرب_الناعمة_القوة_الجاذبة_وأساليب_المواجهة)

[3] - أبو ليلة ،"دور القوة"، مرجع سابق

[4] - Joseph yNe,my softpower, (201)
wttp//www.jstore.org

[5] - ناي، "القوة الناعمة"، مرجع سابق

لقد منح الفضاء الافتراضي الفرصة لإنتشار الأعمال العدائية وممارسة العنف بشكل أوسع و أوضح من ذي قبل و بدون تبعات ولا متابعات قانونية أو قضائية.

المطلب الثالث : النظرية البنائية:

ساهمت أحداث الحادي عشر من سبتمبر في إحياء أفكار المدرسة البنائية والتي عادت أفكارها للظهور بقوة بعد عجز المدارس التقليدية عن تفسير التغيرات الكبرى في السياسة الدولية إثر نهاية الحرب الباردة فقد أدى تفكيك الكيانات القائمة حينئذ ونشوء وظهور كيانات جديدة و ما صاحبه من صراعات مسلحة داخلية على أساس الهوية إلى إعطاء دفعة قوية لأفكارها التي تتمحور حول البناء الإجتماعي للمعاني، بمعنى أن هذه الأخيرة يتم انشاؤها اجتماعيا، فالأفراد يتعرفون على الأشياء المادية ويتعاملون معها وفقا لأفكارهم المشتركة عنها وهكذا تتم عملية تكوين معاني مختلفة لتلك الأشياء وفقا للسياقات الإجتماعية الموجودة فيها.

كما ترى البنائية أن ممارسة القوة تتمثل في إعادة بناء الخطابات و تشكيل الممارسات إذ يعتمد الأفراد على عوامل معرفية لفهم هيكل النظام الدولي و يتم بذلك بناء الحقائق في إطار اجتماعي [1] من خلال تفاعل القيم والهويات والممارسات و بهذا فهي تختلف عن الواقعية و الليبرالية و اللتان تريان أن العالم المادي والأفكار المشتركة عنصران مستقلان عن بعضهما البعض فالمدرسة البنائية تؤمن بتشكيلهما كلا واحدا و هو الاعتقاد الذي أعطى أهمية متزايدة لدور الفواعل غير الدولاتية على صعيد التفاعلات الدولية مما أدى للمضي قدما في تبني القوة الناعمة كمنهج أعتمد عليه منذ تسعينات القرن الماضي ،و مع أنه يبدو للوهلة الأولى أن العسكرة الرقمية تجد أطرها التحليلية في النظرية البنائية التي تعبر عن" كيفية ادراك المجموعات المختلفة لهوياتها ومصالحها" التي مثلت القضية المحورية التي سادت بعد الحرب العالمية الثانية و حتى يومنا هذا[2].

فقد كان للخطاب القدرة على صياغة الكيفية التي يحدد بها الفاعلون الدوليون هويتهم ومصالحهم، وبالتالي تعديل سلوكهم بالغ الأثر في التوجه نحو استخدام الفضاء الرقمي لما توفره بيئته المنفتحة للوصول إلى أكبر قدر من المستخدمين، ولما له من قدرة على تشكيل الصورة الذهنية و الأفكار الثقافية فمثلا موقع أون لاين الذي يستقى منه سكان هونغ كونغ أخبارهم يأتي معظمه من الصين. [3]

نتيجة لما سبق تبقى هذه النظريات قاصرة عن تفسير التفاعلات المختلفة التي تحدث في الفضاء الإلكتروني بسبب استمرار طرحها للدول كوحدات تحليل أساسية أين تقف عاجزة عن تفسير ظاهرة العسكرة الرقمية أين تطغى أهمية الأفكار على أهمية القوة المادية في تشكيل البيانات على عكس الأفكار البنائية.

إن تصاعد دور القوة الالكترونية و التي تعني" مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسب و الشبكات الالكترونية و البنية التحتية المعلوماتية والمهارات البشرية المدربة

---

[1] - جعيجع ،مرجع سابق.

[2] - سارة فندي، "النظرية البنائية في حقل العلاقات الدولية "، الموسوعة الجزائرية للدراسات السياسية و الاستراتيجية(2017)،،آخر تحديث 19 ديسمبر

https://www.politics-dz.com/community/threads/alnzri-albnai-fi-xhql-alylaqat-alduli.105182017 /

[3] - عبد الصادق،"خطر الحروب السيبرانية عبر الفضاء الالكتروني"،(2017)آخر تحديث سبتمبر 2017

http://aitmag.ahram.org.eg/News/83562.aspx

http://aitmag.ahram.org.eg/News/83562.aspx

للتعامل مع هذه الوسائل مشكلة تحديا دوليا بسبب إمكانية تنقلها و انتشارها بين أطراف متعددة منهية بذلك عصر احتكار القوة من طرف الولايات المتحدة الأمريكية بعد أن أسهم الفضاء الرقمي في تدفق المزيد من الفاعلين غير الدوليين و رغم أن البنائيون الذين جادلوا بتأثير الهويات والأفكار والتفاعل بين الوحدات في النظام الدولي ودور ذلك في تحويل الهويات الأنانية أقروا ضمنيا بالأدوار التي تقوم بها هذه الكيانات العابرة للدول غير أنهم يقرون أساسا كما ترى مارثا فيدمورMARTHA FIDMORE[1] بالدور الأساسي الذي تقوم به المنظمات الدولية في ديناميكية التفاعلات الدولية متجاهلين بذلك كليا دور الفرد الذي توليه العسكرة الرقمية نصيبا هاما من الفاعلية على صعيد المسرح الإفتراضي.

المطلب الرابع: النظرية النقدية: مدرسة كوبنهاغن:

اتخذت مدرسة كوبنهاغن من اعتداءات الحادي عشر من ديسمبر مركزا لتطوير تصوراتها الأمنية مما يدل على المرونة التي تتسم بها الأطر التحليلية للنظرية خاصة عند عرضها للأمننة كمعيار محدد للقضايا التي يتم جلها للحيز الأمني لتصنف كتهديد وجودي بناء على تسديدها إذ تعني الأمننة عملية إدخال فكرة و تحويرها عبر وسيلة الاعلام إلى تهديد أمني[2].

و يشكل الفضاء الرقمي بيئة تطبيقية واعدة لأفكار المدرسةالمنادية بايلاء الأفرادأهمية قصوى .

فطبيعة الكيانات المرجعية التي ينظر إليها على أنها مهددة وجوديا وتعدد و تداخل الفواعل الأمنية التي تؤمن لإنشاء مهددات وجودية مع خاصية استعمال الفعل الخطابي والمتمثل في التعابير المستخدمة من قبل الفواعل الأمنية المقبولة من الجمهور جعل من الساحة الالكترونية مجالا واعدا سمح بتطبيق التصورات النقدية لأطرها النظرية فالاستخدامات العسكرية لوسائل الفضاء الالكتروني و أدواته رجحت فكرة دور الخطاب في تشكيل القضايا الأمنية و السياسية،بعدما بات البعد الرقمي يلعب دورا جوهريا في تكوين عناصر القوة وإستمراريتها بفضل تغير معايير القوة التي إرتكز عليها سابقا كالموارد الطبيعية و حجم السكان والمساحة الجغرافية اذ تم إضافة القدرة على استحواذ القوة الرقمية و من ثم القدرة على التحكم و السيطرة على الفضاء الرقمي.

و يلعب الانترنت دورا محوريا في تشكيل قدرة الأطراف المؤثرة على الساحة الدولية خاصة الفرد الذي توليه مدرسة كوبنهاغن أهمية متزايدة على اعتبار تنامي دوره في تشكيل الأحداث الدولية،[3] والذي أتاح له ظهور الفضاء الافتراضي فرصة ممارسة تأثير أكبر مما تتيحه له قدراته المادية سواء الاقتصادية أو العسكرية ،وفي حين تختص الدول بتطوير البيئة الرقمية، يختص الفاعلون غير الدوليون خاصة الفواعل مادون الدول باستهداف ذات البيئة، و يتميزون بصعوبة ملاحقتهم بسبب تعذر كشف هوياتهم.

---

[1] -محمد فرج أنور ،"نظرية الواقعية في العلاقات الدولية "،مرجع سابق

[2] -- مرجع سابق

[3] - محمد مسعد العربي،"من الدولة الى الفرد:تأثيرالسياسات الافتراضية الصاعدة في العلاقات الدولية "،لنازلي شكري،السياسة الدولية (2013)،آخر تحديث20 أكتوبر 2013

http://www.siyassa.org.eg/News/3352.aspx

لقد تميز العصر الالكتروني بمنح الفواعل مادون الدولة بالأخص، القدرة و القوة التي شكلت في نفس الوقت تحديا للأطراف التي كانت تحتكر القوة، ففي حين ترضى الدول بالتنازل عن جزء من سيادتها لفواعل ما فوق الدولة كالمنظمات و الهيئات الدولية، فانه قد شكل استحواذ الفواعل ما دونها كالأفراد و الجماعات المختلفة على القوة تحديا كبيرا لنفوذها خاصة و أن القوة الالكترونية تميزت بالطابع المستتر إذ لا يتم الكشف عن الجاهزية الا عن طريق إجراء المناورات الالكترونية لاختبار القدرات الدفاعية و الهجومية عبر الفضاء السيبراني.و يستغل رواد مدرسة كوبنهاغن ما أحدثته العولمة من تأثيرات في بعض الخصائص السيادية للدول بما كسر احتكار هذه الأخيرة كجزء من الأدوار الأساسية لفائدة "المجتمع المدني " في بعده العالمي وقد ارتبط بهذا المنظور عديد من الاقترابات من قبيل "المجتمع عبر القومي" Transnationalو النظام العالمي Global Regime[1] والتي تعد أكثر استيعابا لواقع تنامي أدوار الفاعلين من غير الدول و تأثيراتهم المتزايدة في السياسة العالمية وهو ما جسدته العسكرة الرقمية بعد أن أتاحت بيئة الفضاء الرقمي المواتية المجال لفواعل ما دون الدولة خاصة لتجاوز التأثير المحلي إلى احداث تأثيرات دولية ، كالمرتزقة الرقميون أو الهاكرز الذين يتخذون من وسائل و أدوات الفضاء الالكتروني أسلحة فتاكة تضرب بها أمن الدول و استقرارها و تسهم في خدمة جهات حكومية معينة .

[1] - أدمام ،"الفواعل العنيفة من غير الدول " ،مرجع سابق

الفصل الثاني :تأثير العسكرة الرقمية على الأمن الدولي

المبحث الأول: الأمن الرقمي : إعادة قراءة في المفهوم التقليدي للأمن

المطلب الأول: مفهوم الأمن الرقمي والبيئة الرقمية

يعتبر الأمن من أصعب المفاهيم التي تناولتها التحليلات المختلفة فكونه مفهوم نسبي متغير ومركب ذو أبعادعديدة و مستويات مختلفة يتعرض لتهديدات مباشرة وغير مباشرة ومن مصادر مختلفة وقد زاد من تعقيد المفهوم دخول البعد الرقمي ضمن أبعاده الغير تقليدية لينتج لنا الأمن الرقمي والذي يعبر عن " مجموع الوسائل التقنية و التنظيمية و الادارية التي يتم استخدامها لمنع الاستخدام غير المصرح به و سوء الاستغلال و استعمال المعلوماتية الالكترونية"[1].

و يعمل الأمن الرقمي على الحماية المعلوماتية للأفراد والهيئات والمنظمات الموجودة في الدولة[2] و تتمثل أهميته في تأمين الحصول على مصادر معلوماتية موثوقة و ذلك بحماية المعلومات الموجودة على الشبكة العنكبوتية. و مع أن مصادر تهديد الأمن محددة ما جعل من تهديدات شتى قضية أمن قومية كونها تهدد المصالح الأساسية اللازمة، فقد تم اعتماد تعريف للأمن القومي بـ " حماية و غياب التهديد لقيم المجتمع الأساسية و غياب الخوف من خطر تعرض هذه القيم للهجوم" و هو التعريف الغير تقليدي للأمن و الذي فرضته التغيرات التي طرأت على مفهوم الأمن عامة بعد انتهاء الحرب الباردة[3]، غير أن ظهور الفضاء الرقمي و تفاقم دوره في بداية هذه الألفية الجديدة فرض اعادة التفكير في مصادر التهديد التي بات الفضاء السيبراني احدهما بصورة تضمن حماية المنشآت اليومية للدولة و البنية التحتية المعلوماتية من الأعمال العدائية من خلال الاستخدام السيئ لتكنلوجيا الاعلام و الاتصال بشكل يجعل من الأمن الرقمي البعد الرابع للأمن.[4]

حسب استطلاع أجري يعتقد 36 % من الخبراء أن الأمن الرقمي أهم بكثير من الدفاع الصاروخي. كما يشير 43 % من الخبراء إلى أن تعطيل الخدمات العامة و الأضرار التي يمكن أن تلحق بالبنى التحتية هو الخطر الأكبر الذي تمثله الهجمات الالكترونية مع كل ما يترتب عن مثل هذا التخريب من أثمان اقتصادية باهضة[5]. و يعبر الأمن الرقمي عن " مجموع الوسائل التقنية

---

[1] - عبير محمد،" الأمن السيبراني" المرسال(2017)آخر تحديث01 نوفمبر2017
https://www.almrsal.com/post/552008

[2] - عبد الاله،"سباق تسلح الكتروني حقيقة واقعة برأي غالبية الخبراء"،ايلاف(2012)،آخر تحديث 01فيفري2012
http://elaph.com/Web/news/2012/2/713508.html

[3] - Nazli Choukri," Cyberpolitics in International Relations" , The MIT Press Cambridge, Massachusetts London, England ,(2012),p 38
https://flavioufabc.files.wordpress.com/2017/02/cyberpolitics-and-international-relations.pdf

[4] -"ما هو الأمن السيراني"، المواطن(2017)، آخر تحديث31 أكتوبر 2017 https://www.almowaten.net/2017/10

[5] - عبد الاله مجيد،"سباق تسلح الكتروني حقيقة واقعة"،مرجع سابق

والتنظيمية و الادارية التي يتم استخدامها لمنع الاستخدام غير المصرح به و سوء الاستغلال و استعمال المعلوماتية الالكترونية".[1]

لقد عانى العالم على مدار السنوات الأخيرة من تهديدات ناشئة أثرت على استقراره وساهمت في خلق المزيد من التوتر في العلاقات ما بين الدول و كانت في مقدمة هذه التهديدات ما تعلق بالاستخدامات العسكرية للفضاء الرقمي عبر الإستغلال الواسع لبيانات الأنترنت الشبكة التي طورت أساسا في بيئة عسكرية لتدعم بالبيئة الأكاديمية.

كما أن أحد أبرز تجليات العولمة اقتران التطور في مفهوم الأمن بالتطور في مفهوم القوة و الفواعل والقضايا و الآليات الدولية المصاحبة و كما انعكست هذه التطورات في التغيرات التي حصلت على مستوى الحركية في الجانب التنظيمي للعلاقات الدولية بداية من النصف الثاني من القرن العشرين،أدت ذات الظروف لتغير البيئة الأمنية خاصة في الفترة ما بعد الحرب الباردة مما استدعى تطوير محاولات تنظيرية هدفت كلها لتوسيع مفهوم الأمن وتعميقه في آن واحد ليشمل ما فوق الدولة وما دونها كوحدات تحليلية معترف بها بل ان التطور الذي شهده قطاع الاتصال و المعلومات أدى لتزايد الدور الذي باتت تلعبه الآليات التكنولوجية نتيجة تزايد الاعتماد على أنظمة وشبكات المعلومات و البني التحتية المعلوماتية لتصبح قضايا أمن المعلومات أحد أبرز القضايا الدولية في العصر الحديث.

بعد دخول تكنولوجيا الإتصالات و المعلومات بكثافة في عمل العديد من المرافق الحيوية حيث ساهمت في تكثيف التفاعلات الدوليةو الذي تجلى في سرعة انتقال الأفكار و الأموال و الأفراد بين دول العالم حيث وصل عدد مستخدمي الانترنت إلى 2.1 مليار مستخدم و 2.4 مليار مستخدم للشبكات الإجتماعية و 3.146 مليار حساب بريدي مفتوح بالاضافة إلى 5.9 مليار مستخدم للمحمول و بليار فيدو تم فتحه من اليوتيوب الشيء الذي عزز من انتشار الأنشطة غير السلمية للفضاء الالكتروني الذي يتجاوز الحدود الدولية خاصة و أن الفضاء الرقمي يواجه تهديدات متصاعدة نتيجة البيئة الأمنية الجديدة التي ساهم في تشكيلها.

تميزت البيئة الأمنية الجديدة بجملة من الخصائص ك:

1- هشاشة البيئة الكونية التحتية المعلوماتية بفعل ظهور المعلومات الالكترونية و المدن الذكية مما زاد من احتماليات تعرضها للخطر.
2- انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص و خاصة المنشآت الحيوية.
3- تصاعد دور الشركات المتعددة الجنسيات و التي أصبحت قدراتها تفوق قدرات الدول مثل مواقع الشبكات الإجتماعية فيس بوك و تويتر و اليوتيوب و الذين تحولوا لفاعلين دوليين جد مؤثرين.
4- التنافس التكنلوجي في عمليات الانتاج و الابتكار.
5- الأهمية المتزايدة للاتصالات كأحد أوجه الأمن.
6- إعادة النظر في تعريف الأمن مع عدم كفاية الاعتماد على القوة العسكرية لحماية الأمن القومي.
7- اتجاه الصراع الدولي حول الموارد و المصالح و القيم نحو الاعتماد على تكنولوجيا الاتصال و المعلومات.

---

[1] - "دليل الأمن السيبراني للدول النامية "،الاتحاد الدولي للاتصالات(2006)
https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf

8- التنافس في ساحة الانجازات ذات الطبيعة المادية و بروز صراعات الأفكار و القيم.[1]
9- انتقال الصراعات الممتدة عبر الفضاء الرقمي كتكرر حالات القرصنة المتبادلة دون أن تسفر عنها حرب تقليدية بالضرورة مثل حالة الصراع مابين الهند و باكستان أو الصين و كوسوفا و غيرها.
10- صعود دور الفرد في العلاقات الدولية.
11- استخدام الفضاء الرقمي كوسيلة من وسائل الصراع الطائفي أو الديني أو العرقي مما ساعد على كشف ديناميات التفاعل الداخلي إلى الخارج العامل الذي سهل عملية الاختراق الخارجي، و هي العملية التي تتم عبر شبكات الاتصال و ذلك بدعم أحد أطراف الصراع بأدوات غير قتالية.

-الدور الفعال الذي تلعبه عسكرة الفضاء الرقمي في ادارة الصراع السياسي بين الشركات التكنولوجية الكبرى و الدول من ناحية، و ما بين النظم الحاكمة و الحركات المعارضة لها من ناحية أخرى، حيث برز تفاوت في استخدامات الفضاء الرقمي وفق طبيعة التطور التقني وقدرة النظام على ادارة الصراع الاعلامي و التأثير في الرأي العام و تعبئة وحشد الجمهور، فقد نجح النظام السوري مثلا في ادارة معاركه بالأفكار المضادة و الاختراقات المتبادلة في حين فشل النظام المصري في استخدام الفضاء في ادارة ازمة الاحتجاجات خاصة بعد قطع خدمة الانترنت والإتصالات، بينما لم تستطع ليبيا و اليمن استخدامه و اكتفت بتحريك القوة الصلبة عوضا عن الناعمة.

-زعزعة استقرار المجتمعات عن طريق شن الحرب النفسية التي يعد الفضاء الرقمي أفضل و سيلة لها بسبب اتاحته امام الجميع و تمكنه من خلق شعور لدى الشعب بعدم الثقة في مؤسسات الدولة.

المطلب الثاني: تداعيات البيئة الأمنية الجديدة

ساعدت البيئة المحلية والسياق الدولي للفضاء الرقمي ببروز صراعات ذات بعد محلي ودولي وذلك من خلال ايجاد بيئة مناسبة تدمج القوى والفئات المهمشة في السياسة الدولية و قد صرح باراك أوباما الرئيس الأمريكي السابق أن " مخاطر الأمن الالكتروني تشغل جزءا من أخطر تحديات القرن الواحد و العشرين و التي تهدد الإقتصاد و الأمن القومي للدول ".وهي نفس تصريحات عدد من قادة الدول مثل بريطأنيا و الصين الذين اعربوا عن ما يسمى بـــ " القلق التكنولوجي"[2] من تلك الارقام الصاعقة التي تقود إلى نطاق واسع من التهديدات، فبعد دخول تكنولوجيا الاتصال الساحة العسكرية انحسر دور الدولة مقابل تصاعد دور الفاعلين من غير الدول في العلاقات الدولية كالشركات التكنولوجية العابرة للحدود و شبكات الجريمة و القرصنة الإلكترونية و الجمعات الارهابية و القراصنة وأضحى الامن المعلوماتي من متطلبات الحفاظ على الأمن الوطني والقومي أمام تراجع سيادة الدولة مما أدى بهذه الأخيرة لتبني استراتيجيات خاصة لحرب المعلومات و الاستعداد لحرب المستقبل، و هي استراتيجية مزدوجة لا تبنى على امتلاك القوة فقط و انما على القدرة على شلها أيضا باستهداف منشآت حيوية.

و تسعى الدول في هذا الصدد لتحديث قدراتها الدفاعية و الهجومية و ذلك بالاستثمار في البنية التحتية للمعلومات و تأسيسها بتحديث القدرات العسكرية و تكثيف برامج التدريب بغرض رفع

---

[1] - عبد الصادق ،" عسكرة الفضاء الالكتروني "،مرجع سابق
[2] -عبد الصادق،" الفضاء الالكتروني و أسلحة الانتشار الشامل" ،مرجع سابق

الجاهزية، ورفع القدرات البشرية داخل الأجهزة الوطنية المعنية، ان سوء استخدام الفضاء الرقمي أدى إلى خلق ما يسمى الأمن الرقمي و الذي تطلب عددا من الاجراءات المتعلقة بما يلي:

- التأكد من سلاسة الدفاعات الرقمية و عدم تعرضها لأي خلل فني طارئ وما يستلزم ذلك من ادماج هذا في الاستراتيجية الشاملة للدفاع للدول بطريقة تشكل ردعا رقميا و هي الاستراتيجية التي تطبقها اسرائيل بنجاح.

و حذت الدول حذوها بتحديث الجيوش و تدشين وحدات متخصصة في الحروب الرقمية و اقامة أقسام خاصة بالدفاع الالكتروني و القيام بالتدريبات و المناورات و اقرار مشروعات وطنية للأمن الرقمي القومي.

- طبيعة الفضاء الرقمي كساحة عالمية عابرة للحدود الوطنية جعل الأمن القومي السيبراني يمتد من داخل الدولة إلى النظام الدولي مشكلا نوعا من الأمن الجماعي العالمي بالنظر للخطر المشترك الذي يهدد مجتمع المعلومات العالمي.

- الطبيعة المتغيرة للتفاعلات الدولية أوجدت مصلحة دولية في التصدي لهذا النوع من التهديد[1] .

- الاستخدام الغير السلمي للرقمنة أثر في الاستقرار السياسي و الإجتماعي للدول و تحول لسبب مباشر يهدد العلاقات الدولية مسبب قوي لحدوث أزمات دولية عدة كفضيحة تسريب المعلومات لوكالة ويكيليكس.

- زعزعة ثقة الحلفاء بعضهم ببعض اثر عمليات التجسس الواسعة التي سهل من حدوثها الأدوات المتطورة التي يوفرها الأمن الرقمي.

- تغير ميزان القوى العالمي بشكل سريع بعد انتهاء عصر احتكار القوة وصعود دول أو فواعل لآداء وظائف تساهم في صنع القرار الدولي.

- تعزيز فكرة الفضاء الرقمي لما يسمى "بالقوة المؤسسية" في السياسة الدولية[2].

- اعادة توزيع القوة او اعادة نقلها بين الأطراف المسببة.

- انتشار القوة بشكل سريع بين أطراف متعددة مما يعمل على انهاء احتكارها من طرف قوة واحدة.

---

[1] - عبد الصادق،" الفضاء الالكتروني و أسلحة الانتشار الشامل" ،مرجع سابق

[2] -عبد الصادق ،"خطر الحروب السيبرانية"،مرجع سابق

المبحث الثالث: تأثير على مستوى التهديدات

يستهدف الأمن الرقمي تهديدات شتى منها ما يتسم بالطابع المرن كالتجسس و الحرب المعلوماتية التي تبرع فيها أجهزة الاستخبارات الدولية من أجل دعم أنشطتها السرية وجمع المعلومات من مناطق الاستهداف بغرض معرفة توجيهات الرأي العام في الدول المختلفة و الاحاطة بتوجهات القادة و الزعماء و النخب و سائر دوائر صنع القرار كما تتخذ أخرى طابعا صلبا بسبب شكلها التخريبي و التدميري كالهجمات الالكترونية و الحروب السيبرانية. ويمكن تصنيف تهديدات الأمن الرقمي في مستويات عدّة نذكرها كالآتي:

المطلب الأول: سباق التسلح الرقمي

إذا كانت الحرب العالمية الأولى اندلعت بسبب "اطلاق النار في جميع انحاء العالم، ونيران الحرب النازية المتداعية في بولندا أشعلت نار الحرب العالمية الثانية فمن المرجح أن تكون بداية الحريق العالمي التالي هادئة مثل نقرة فأرة"[1].

ان العمل على اختراق الأمن القومي للدول دون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السياسية أصبح ممكنا بعد أن أصبح الصراع الدولي صراعا رقميا يأخذ طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي الدولي وسرقة الأسرار الاقتصادية و العلمية و يمتد الصراع إلى أسماء و عناوين المواقع و التحكم في المعلومات و ذلك باستخدام الهجمات الرقمية والتجسس الالكتروني واستهداف الاقتصاد لشل قدرات الدول الدفاعية. ان تصاعد الهجمات الالكترونية بشكل مضطرد يدفع بالدول بشكل متزايد وسريع نحو سباق تسلح رقمي خطير قد يجر نحو خطر الانزلاق في حرب سيبرانية بالنظر إلى شراسة المواجهة الدائرة بين أطراف الخصام في الفضاء الإلكتروني.

و تعمد الدول بهدف رفع قدراتها في مجال التسلح الرقمي بالاستثمار فيه، مما يعكس سعي الدول الحثيث لتحقيق أكبر قدر ممكن من التفوق[2] في مجال لم يتم اختباره بعد بشكل واضح، يحكمه الخوف وعدم اليقين ويهدد بنشوب حرب تدخل ضمن حروب الجيل الخامس[3]، بعد أن عمدت أكثر من 400 دولة تحوز قدرات قتالية عسكرية نظامية رقمية هائلة، حيث تجهز فرنسا جيشا من المتسللين الالكترونيين القادرين على شن هجمات مضادة، و هو ما يفسر زيادة ميزنيات الانفاق في وزارة الدفاع التي عمدت لتجهيز الجيش الرابع المقدرة بمليار يورو في شكل استثمار مبدئي حتى عام 2019، الهدف منه تجهيز 32200 جندي مع الابقاء على قوة احتياطية قوامها 4400 جندي.

---

[1]Dennis F Poindexter,
"the new cyberwar :technology and redifinition of Warfare " , copyrited Material(2013), 12-13
https://www.amazon.com/New-Cyberwar-Technology-Redefinition-Warfare/dp/0786498439

2- عبد الصادق ،"الفضاء الالكتروني و أسلحة الانتشار الشامل"،مرجع سابق
[3] - مروة الاسدي،"سباق التجسس الالكتروني و زعزعة النظام العالمي"،جريدة الاعلامي (2018)، آخر تحديث 26/01/201
http://www.themediamagazine.com/ArticleDetail.aspx?id=9990

وغير خفي أن مسألة التسريبات كالتي قام بها موقع ويكيليكس ساهمت بشدة في تأجيج الوضع الدولي بعد أن تم كشف قدرة المخابرات الأمريكية على اختراق جميع الأجهزة الإلكترونية التي تصنعها شركات صينية، أما روسيا فهي بصدد انشاء قوة "الحرب المعلومات " و هي الخطوة التي من شأنها رفع درجة مخاوف الغرب، اذ حسب وزير الدفاع الروسي سيرغي شويغو فإن على الدعاية أن تتسم بالذكاء والفعالية، وتكون قادرة على المنافسة، وهي التصريحات التي تؤكد على استخدام روسيا " لوسائل سوفياتية" للتأثير على الرأي العام. وفي خطوة لمواجهة الدعاية الكاذبة قامت الدول الغربية بتعزيز قوات حلف شمال الأطلسي في دول البلطيق قرب حدودها الغربية،أما فيما يخص مواجهة الانتهاكات الكورية فقد عمدت الدول الغربية الى مضاعفة الاجراءات العسكرية و التدابير التقليدية الا أن هذا لم يتمنع كوريا الشمالية من استهداف بنوك لازاروس و مؤسسات مختلفة في 31 دولة اذا استطاعت جماعة كورية سرقة 31 مليون دولار من بنك بنغلاديش المركزي واستهدفت شركة سوني بيكتشرز فضلا عن الحملات طويلة الأمد المستخدمةمن طرف منظمات كثيرة في كوريا الجنوبية.

ويعتبر الأمن الالكتروني مبعث قلق كبير لبرلين اذ تسعى ألمانيا الاتحادية خاصة في الفترات الانتخابية لرفع جاهزيتها الدفاعية مما دفع لانشاء قيادة جديدة للأمن الالكتروني،و تقسم الحكومة المسؤوليات بين الجيش ووزارة الداخلية المسؤولة عن الهجمات الرقمية الداخلية كما تعمل القيادة الألمانية[1] على دمج القيادة العسكرية الحالية للاستطلاع الإستراتيجي، ومراكز الإتصال الخاصة بالعمليات والمعلومات الجغرافية.

وهو ما يعني اعتماد السلاح السيبراني كسلاح سادس رئيسي في الجيش بجانب البحرية و سلاح الجو و الخدمات الطبية و الأركان المشتركة و اعتبار حماية البنية الحساسة الألمانية من الهجمات الرقمية المحتملة كأولوية قصوى.

المطلب الثاني :القرصنة الالكترونية

أولا: تعريف القرصنة الالكترونية

تمثل القرصنة الالكترونية أو الرقمية " عملية اختراق أجهزة الحاسوب " و التي تتم عبر شبكة الانترنت غالبا بما أن أغلب حواسيب العالم مرتبطة بهذه الشبكة أو حتى عبر شبكات داخلية يرتبط بها أكثر من جهاز حاسوب يقوم بها شخص أو عدة أشخاص متمكنين في برامج الحاسوب و طرق ادارتها، وهم مبرمجون ذوو مستوى عالي يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين و التعرف على محتوياته و من خلالها اختراق الأجهزة المرتبطة معه في نفس الشبكة[2].

وتعرف القرصنة الالكترونية بلغة القانون أنها " كل شكل من أشكال الاعتداء على المنتجات الفكرية و المصنفات الرقمية و الحصول على نسخة منها دون موافقة صاحبها" و تقسم إلى فئتين:

-فئة اتصال البرمجيات و تشمل عمليات النسخ الكلي أو الجزئي.

---

[1] - مروة الاسدي،"سباق التسلح الالكتروني "، النبأ(2018)
annabaa.org/Arabic/information/105-89
4-كريم حميدة ،"القرصنة الالكترونية"، الألوكة الثقافية (2013)،آخر تحديث 04 أفريل 2013
www.alakah.net/aulture/0/52639/

-فئة البرامج الشاملة التي تطال شبكة الانترنت و ما تحويه من بيانات : مدخلات ومخرجات أو مخزنة.

وللقرصنة الالكترونية عدة أشكال منها:

1-القرصنة الهاتفية: تحول علب الكترونية دون عمل معدات احتساب المكالمة و هذا يتم عن طريق اجراء مكالمات هاتفية دون تسديد أجرها.

2-قرصنة البرامج المحلية: وتعني تجاوز البرمجيات التي توضع للحؤول دون اختلاس نسخ البرامج الحاسوبية التطبيقية أي بصورة غير مؤذية.
ولتجنب آثار القرصنة الإلكترونية يجب:
- عدم فتح أي رسالة الكترونية مجهولة المصدر لأن الهاكرز يستخدمون رسائل البريد الالكتروني للتجسس.
- عدم الدخول إلى المواقع المشبوهة كمواقع التجسس و المواقع التي تحارب الحكومات و المواقع الاباحية لأن الهاكرز يستخدمها لتنصيب ملف التجسس (الباتش) تلقائيا بمجرد دخول الشخص للموقع.

- استخدام برامج الحماية من الفيروسات و القيام بالمسح الدوري و الشامل للجهاز.

يستهدف الهاكرز المصارف لسحب الأموال أو المواقع الأمنية الحساسة للدول بغرض التلاعب ببياناتها أو تدميرها. ويستطيع الهاكرز اختراق مواقع الشركات و فك كلمة السر الخاصة بالبريد الالكتروني أو موقع الشركة على الانترنت أو فك " السيريال نمبر" عند تثبيت البرنامج. ومن أشهر الهاكرز:

-فلادمير ليفين Vladimine Levin : روسي استطاع استدراج حاسبات "سيتيتبانك" إلى اعطائه 10 مليون دولار.

- يوهان هيلسينجيوس Johan Helsingins:وهو معروف بإنشاء رسائل البريد الالكتروني المشهور و المسمى بـــ "بنت.في" (pent fi) .[1]

- كيفين ديفيد ميتنيكKevin David Mitnick **:يعرف** باسم " كوندور" condor كشهرة له على الشبكة، و رغم أنه لم يتعدى سن المراهقة الا أنه استعمل غرف المحادثة في الانترنت لارسال رسائل لأصدقائه، و يعتبر أول قرصان يكتب اسمه في لوائح الأف بي أي FBI بين المجرمين الأكثر طلبا[2].

ومن أهم عمليات القرصنة الإلكترونية التي حدثت:

---

[1] - كريم حميدة ،"القرصنة الالكترونية"، مرجع سابق

[2] - كريم حميدة ،"القرصنة الالكترونية"،مرجع سابق

1- تمكن عام 1986 "روبيرتو سوتو" وهو كولمبي الجنسية من سرقة تيليكس حكومي حيث أرسل عبره مجموعة رسائل إلى عدد من المصارف في المملكة المتحدة و قد نتجت عن هذه العملية نقل 13.5 مليون دولار من أرصدة الحكومة الكولمبية.
2- كما استطاع أحد طلاب جامعة كورل زراعة برنامج worm في شبكة حواسيب حكومية انتشر خلال 6000 حاسوب و تسبب في خسائر كبيرة مما أدى لايقافه و تغريمه بمبلغ 6000 دولار[1].
3- عام 1994 قامت مجموعة من القراصنة الروس بنقل 10 ملايين دولار من City Bank إلى حسابات مصرفية في مختلف دول العالم حيث كان زعيم العصابة "فلادمير ليفين" يستخدم حاسوبه الشخصي لتحويل الأموال إلى حسابات في فنلندا و اسرائيل حتى تم ايقافه في الولايات المتحدة و تقديمه للمحاكمة.
4- خلال عام 1995 تعرضت المواقع الفدرالية للولايات المتحدة للتشويش كما استهدفت حواسيب وزارة الدفاع الأمريكية بـــ 250.000 هجمة.
5- اخترقت مجموعة من قراصنة الموقع الالكتروني لشركة مايكروسفت للبرمجيات عام 2001 وتوقف تصفح الموقع لمدة يومين كاملين.
6- سنة 2007 قام قرصان تركي بالهجوم على موقع منظمة الأمم المتحدة على شبكة الانترنت حيث نسخ البرامج الحاسوبية الغربية و أعاد تصديرها لدول أوروبا الشرقية.[2]

المطلب الثالث: الجريمة السيرانية المنظمة:

رغم أنه لا يوجد تعريف محدد و متفق عليه للجريمة السيبرانية الا أنها تعتبر نشاطا غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة على حاسوب معين بغير اذن صاحبه و يمكن تصنيفها بين جريمة سيبيرانية داخلية و أخرى خارجية، و تؤكد المحاولات القليلة لتعريفها على أنها سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات " و تتعدد آليات الجرم الرقمي بين:

-التنصيب على الهواتف

-سرقة الوثائق العسكرية

-تسريب بيانات المواطنين

وتعد المنظمات الاجرامية أحد الفواعل التي تخل بالتوازن الدولي و التي غالبا ما تقوم بحمايتها ورعاية مصالحها عدد من الحكومات الضعيفة و الفاسدة.

وقد استطاعت الجماعات الاجرامية المنظمة تحديث نشاطاتها الغير قانونية خاصة منها اختراق شبكات البنوك بغرض تحويل الأرصدة و سرقة المعلومات الهامة واختلاس حسابات أعضائها عبر القيام بانشاء أسواق سوداء على الانترنت لبيع المعلومات المالية خاصة و المتعلقة بكلمات المرور الشخصية و الحسابات البنكية و أرقام بطاقات الائتمان، و بلغ معدل نشاطها سقفا عاليا حيث تكلف الجرائم الالكترونية الشركات أكثر من تريليون دولار سنويا بسبب صعوبة التصدي لها

---

[1] - سارة حمدي ،"تعرف على 11أخطر هاكر في العالم بينهم مصري"، صوت الأمة (2017)،آخر تحديث30 ديسمبر 2015 http://www.soutalomma.com/Article/79284/

[2]- مرجع سابق

مع عدم تمكن المحققين من كشف هوية هذه المنظمات لما يسمح به الفضاء الالكتروني من قابلية للتخطي، لذا فصعوبة مراقبة نشاطاتها أدى لازدهار أعمالها في ظل استحالة تتبع أفرادها من أجل تقديمهم للمحاكمة ويقدر التقرير الصادر عن شركة نورتون Norton للأمن الالكتروني لعام 2011 أن 431 مليون شخص يتعرضون سنويا للجريمة الالكترونية كما يقع يوميا أكثر من مليون شخص ضحية للجرائم الالكترونية ، ويوضح التقرير أن 64% من الأشخاص الذين يقضون ما بين ساعة إلى 24 ساعة في الأسبوع مع الانترنت يكونون عرضة للجرائم الرقمية[1].و ما يميز الجرائم الالكترونية عن غيرها من أشكال سوء استخدام الفضاء الرقمي هو استهداف قراصنتها للشركات الخاصة في غالب الأحيان الا في حالات نادرة أين تستهدف المؤسسات الحكومية و يكون ذلك في الأغلب تلبية لجهات دولية معينة و تتم الصفقات المالية بشكل يخلي المؤسسات الحكومية من المسؤولية الدولية عن الاعتداء الرقمي الذي تستهدف منه المنظمة الاجرامية المنفعة المادية بشكل أساسي اذ يضل الدافع الأول لتحركاتها و الهدف من وراء نشاطاتها هو الربح المادي أولا و أخيرا[2].

جدول يوضح التوزيع العالمى لهجمات مواقع الإنترنت[3]

((Global Distribution of Website Attackers.

Top	USA	China	UK	Israel	Brazil	Russian Federation	Indonesia	Germany	Pakistan
Glob	48. 80%	20.98%	9.19%	2.15%	1.27%	0.97%	0.91%	0.84%	0.74%

الم

المصدر :نسرين الشحات الصباحي علي،"الأبعادالعسكرية للقوة السيبرانية على الأمن القومي للدول"،المركز العربي الديموقراطي للدراسات الاستراتيجية و الاقتصادية و السياسية(2016) https://democraticac.de/?p=30962

المطلب الرابع:الإرهاب الرقمي:

[1] -اسراء جبريل رشاد مرعي،"الجرائم الالكترونية: الأهداف- الأسباب- طرق الجريمة و معالجتها"،المركز الديموقراطي العربي للدراسات الاستراتيجية و الاقتصادية و السياسية(2016)،آخر تحديث 09 اوت 2016 https://democraticac.de/?p=35426

[2] - مرعي ،"الجرائم الالكترونية"،مرجع سابق

[3] - الشحات،"أبعاد القوة"،مرجع سابق

أولا: تعريف الارهاب الرقمي

ظهور الارهاب الرقمي تعلق بأحداث الحادي عشر من سبتمبر 2001 حينما وجد العمل الارهابي في الفضاء الرقمي مجالا جديدا لنقل نشاطاته الدموية. وتعتبر بعض الدراسات ممارسة القوة عبر الأنترنت اذا ما صاحبتها دوافع سياسة مثل التأثير على القرارات الحكومية أو الرأي العام[1].

غير أن هذا المصطلح الذي يستخدم أساسا لوصف الهجمات غير الشرعية التي تنفذها المجموعات أو الفاعلون غير الحكوميون. ولا يمكن تعريف أي هجوم رقمي بأنه إرهاب رقمي الا إذا انطوى على نتائج تؤدي إلى أذى مادي للأشخاص أو الممتلكات وإلى خراب يترك قدرا كبيرا من الخوف.

أما حسب تعريف دينينج فالارهاب الرقمي هو " التقاء الارهاب بعالم الكمبيوتر"، وقد كان لظهور الارهاب الرقمي الأثر الأهم على انهاء عصر احتكار القوة بعد أن ثبت أن امتلاك القوة لم تعد مقصورة على الدول الكبرى بل لكل من كانت له القدرة على امتلاك المعرفة التكنولوجية و كذا القدرة على توظيفها بهدف تحقيق أهداف استراتيجية معينة للدول للفاعلين من غير الدول[2]، ويقوم الارهاب الرقمي على على ركيزتين اثنين:

- العمل على تدعيم العمل الارهابي المادي بتوفير المعلومات و الأماكن المستهدفة أو العمل كوسيط في تنفيذ العمليات الارهابية.
  شن حرب الأفكار و ذلك بالتحريض على بث الكراهية الدينية و الفكرية.

ان الهدف من الارهاب الرقمي أساسا هو استخدام الانترنت لتضخيم الصور الذهنية لقوة و حجم المنظمات و الجماعات الارهابية حتى أنها شكلت خلايا اعلامية رقمية و جندت مختصين لخدمة الجانب الاعلامي العسكري بغرض الوصول إلى المعلومات و الحصول على التمويل و التبرعات و حشد الأتباع فضلا عن تبادل الأفكار و التنسيق للعمل الارهابي.

وتوصلت إلى تدمير مواقع الانترنت المضادة و اختراق المؤسسات الحيوية و تعطيل الخدمات الحكومية الرقمية كمحطات للطاقة الأمنية في تفتيش و القضاء على الجماعات الارهابية التقليدية.

و تتمثل أهم أهدافه في التبعية و التجنيد و استقدام العناصر الجديدة مستغلين تعاطف الآخرين[3] من مستخدمي الانترنت خاصة و أن الفئة المستهدفة عادة ما تكون الشباب و المراهقين الأكثر ولعا بالانترنت، غير أن التخطيط و التنسيق يظل الهدف الأول بعد أن أصبحت شبكة الأنترنت وسيلة بالغة الأهمية بالنسبة للمنظمات الارهابية حيث تتيح فرصة تنسيق الهجمات الرقمية و تحديد المهام الخاصة بكل عنصر ارهابي من عناصر المجموعة، و بالمقابل تمخض عن هذا الاتجاه الجديد في الاعتداء تطور أساليب دفاعية جديدة لدى الدول المستهدفة اذ عمدت لانشاء أجهزة خاصة باختراق

[1] -- محمد مبارك البنداري ،"الارهاب الالكتروني مفهومه ووسائل مكافحته"، شبكة ضياء (2014)،آخر تحديث 29أكتوبر 2014 https://diae.net/16243

[2] -ريهام عبد الرحمان رشاد العباسي، "أثر الارهاب الرقمي الالكتروني على تغيير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية". المركز الديمقراطي العربي(2016)،آخر تحديث 24 جويلية 2016

p?/de.democraticac//:ttpsh=34528

[3] -العباسي،"أثر الارهاب الالكتروني"،مرجع سابق

الجماعات الارهابية عبر التسلل إلى أنظمتها و التجسس على اتصالاتها و حتى تجنيد بعض عناصر الأمن للعمل متخفين داخلها بهدف القضاء عليها من الداخل.

و يعد هجوم الحادي عشر من سبتمبر 2001 من أكبر الهجمات الارهابية التي تثبت اعتماد منظمة القاعدة البارزين على الانترنت في التخطيط لها. اذ يعتبر هذا التاريخ نقطة تحول مهمة في تفطن الدول لخطورة عسكرة الفضاء الرقمي و اتخاذها الاجراءات الحادة بشأن التعامل مع التوجه الرقمي العسكري الحديث. كما أن خطر الارهاب الرقمي يكمن في سهولة استخدام هذا السلاح مع شدة أثره خاصة و أن أكبر الجهات استهدافا هي المنظمات و المؤسسات الأمنية.[1]

و قد وعت الجماعات المتطرفة أهمية و فعالية السلاح الرقمي منذ أمد طويل اذ يعد Tom Metzager وهو أشهر المتطرفين الأمركيين العنصريين و مؤسس جماعة المقاومة "الأربانية البيضاء" white aryam resistance من أوائل من أسسوا مجموعة بريد الكترونية ليتواصل مع أتباعه و يبث أفكاره العنصرية عام 1975 قبل حتى أن تظهر شبكة الانترنت[2].

ثانيا :خصائص الارهاب الرقمي

هناك جملة من الخصائص تلك التي تميز الارهاب الرقمي عن الارهاب العادي:

- كونه عملا اجراميا عابرا للحدود و هو ما دفع الدول لمحاولة تنسيق جهودها الرقمية الدفاعية و التعاون فيما بينها.

- صعوبة اكتشاف جرائم الارهاب الرقمي بسبب نقص خبرة الأجهزة الأمنية في هذا المجال و كذلك يعود الأمر لغياب الأدلة المادية وسهولة اتلافها و تدميرها[3].

- خبرة مرتكبيه بمجال تقنية المعلومات، و قد أفرزت سهولة الاتصال و امكانية التنسيق عبر الشبكة العنكبوتية العالمية سمة جديدة للجماعات الارهابية وهو عدم وجود زعيم ظاهر للجماعة مما غير من نمط المواجهة وجعل من الصعوية بمكان القضاء عليها عبر بتر رأسها أو تحطيم الهرم من أعلاه و هو الأسلوب الذي كان متبعا من طرف الأجهزة الأمنية .[4]

ثالثا :أساليب الدول المنتهجة لمكافحة الارهاب الرقمي

---

[1] -م. م حوراء رشيد مهدي الياسري،"الارهاب الالكتروني وطرق مواجهته "،مركز الفرات(2017)،آخر تحديث 25 ماي 2017
http://fcdrs.com/polotics/766

[2] - علي عدنان الفيل ، الارهاب الالكتروني " مجلة الجامعة الخليجية ،(العراق :جامعة الموصل ،كلية الحقوق ،مجلة الجامعة الخليجية ،العدد الثاني،2010
files/com.almanhal.formplat//:ttpsh/2 /7983

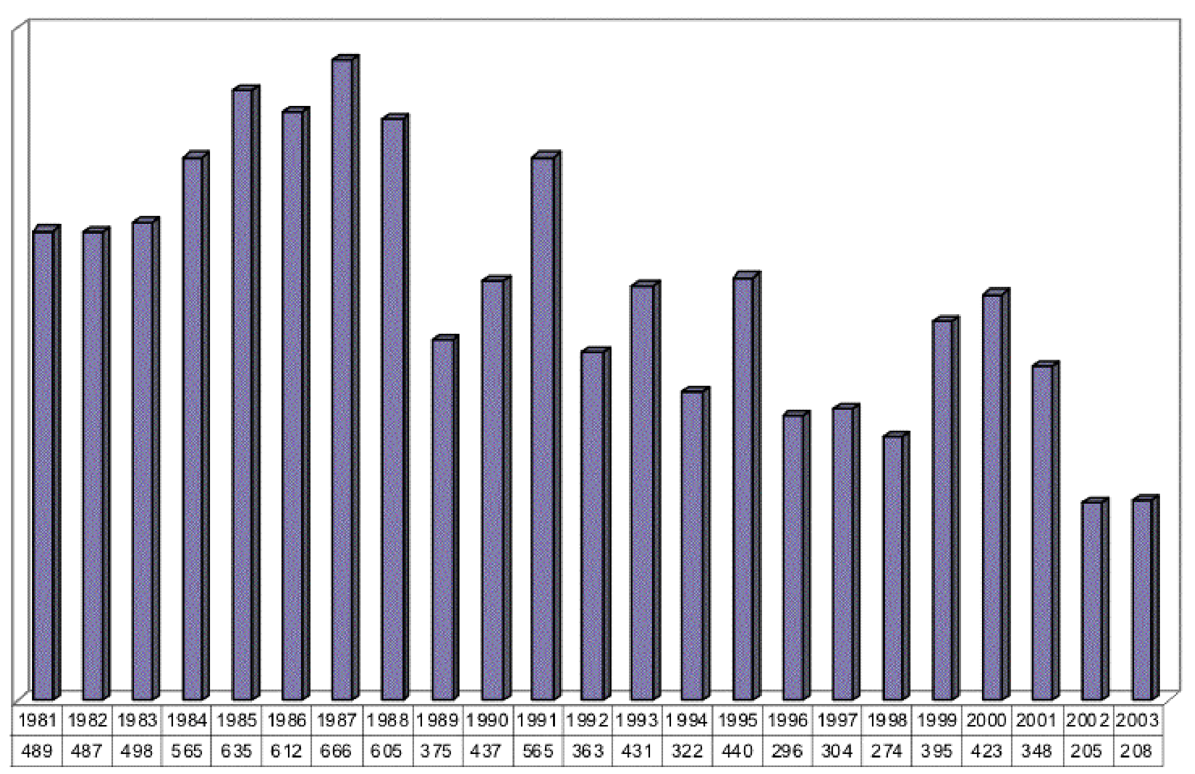
[3] - ذياب موسى البداينة ،"الارهاب المعلوماتي" (ورقة مقدمة للحلقة العلمية حول الانترنت و الارهاب، جامعة نايف العربية للعلوم الأمنية ، 15 -19 نوفمبر 2008) أطلع عليه بتاريخ 16 أفريل 2018

https://repository.nauss.edu.sa/bitstream/handle/123456789/56415ا.pdf?sequence=1&isAllowed=y

[4] - "الارهاب الالكتروني و طرق مواجهته " ،شبكة النبأ المعلوماتية (2010)
informatics/arabic/org.annaba//:https/11123

- الاعلام المضاد و الموجه ضد الجماعات المتطرفة أو ابراز دور الأجهزة الأمنية في مكافحته بغية تعزيز ثقة الجمهور في قدرة أجهزة الدولة.
- تعظيم دور المواطن في التصدي لجرائم الارهاب من حيث كونه الفئة الأولى المستهدفة به.
- رصد ومتابعة المواقع الرقمية المشبوهة من خلال انشاء فرق و اقسام متخصصة بقضايا الارهاب الرقمي بالاضافة إلى:
- تعزيز التعاون الاقليمي و الدولي في متابعة ورصد نشاط هذه المواقع المشبوهة.
- ضرب اتصالات القيادات بروابطها لتخفيف مصادرها البشرية و المالية و الفكرية.

وأخيراً فان مكافحة الارهاب الرقمي تستلزم وضع خطط استراتيجية شاملة تتضمن بناء مؤسسات دولية في اطار القطاعين الخاص و العام.[1]



[1] -- ذياب موسى البداينة ،"الارهاب المعلوماتي "(2008)،اطلع عليه بتاريخ 06 ماي 2018

https://repository.nauss.edu.sa/bitstream/handle/123456789/56415/.pdf?sequence=1&isAllowed=y

منحنى بياني يوضح عدد الحوادث الارهابية للفترة 1981-2003[1]

- المصدر:ذياب موسى البداينة ،"الارهاب المعلوماتي "(2008)،اطلع علبه بتاريخ 06 ماي 2018

https://repository.nauss.edu.sa/bitstream/handle/123456789/56415/.pdf?sequence=1&isAllowed=y

المبحث الثالث :تأثير على مستوى الوسائل

يمكن الجزم بلا أدنى شك على أن العسكرة الرقمية أثرت بشكل بالغ على الوسائل التي تعتمدها الدول بغية تحقيق الأمن الدولي في ظل عدم جدوى فعالية الوسائل التقليدية لمواجهة التحديات المستجدة على صعيد الفضاء الرقمي و التي استدعت أنماطا جديدة للمواجهة.

المطلب الأول: الردع الرقمي

تعتبر نظرية الردع إحدى نظريات إدارة الصراع التي تستند أساساً على الأدوات العسكرية ، لذلك كثيراً ما يقرن البعض مصطلح الاستراتيجية بمصطلح الردع، لذا بات مصطلح "إستراتيجية الردع" من المصطلحات شائعة الاستخدام سواء في مجال التخطيط العسكري أو العلاقات الدولية.

وتستند نظرية الردع على افتراض مفاده أن القوة هي أفضل علاج للقوة، فقوة الدولة هي العامل الأساسي لكبح جماح الآخرين، فعندما يتحقق لدولة ما تفوق في القوة فإنها تستطيع فرض إرادتها على الدول الأخرى، ولا يكبح جماحها إلا قوة أخرى مضادة لها أو متفوقة عليها، وهو ما تبنى عليه سياسة الردع أو ردع القوة. وبرغم أن سياسة الردع التي تتبعها الدول قد تشكل عاملاً من عوامل الصراع بقدر كونها وسيلة لتجنب الصراع، إلا أنه في حالة وجود صراع وحدثت مواجهة بين أطرافه فمن المؤكد أن هذا التهديد سوف يتضاعف إذا ما واجهت القوة ضعفاً، فتقصير الدولة في تعزيز قوتها هو حكم عليها بالهلاك لأنها تشجع غيرها بالعدوان عليها

أولا :تعريف الردع الرقمي

اعتمادا على القاعدة الأساسية للردع و التي تفيد بأنه كلما زادت القوة التدميرية للسلاح كلما قل استخدامه و هي القاعدة التي استقيت من النموذج التقليدي للردع الأ ول و هو الردع النووي، و بما أن الدول النووية الكبرى لا تتوفر على ميل لاستخدام او حتى التلويح بالسلاح النووي كوسيلة لتسوية نزاعاتها و صراعاتها القائمة تجنبا منها للدمار الحتمي المتبادل[2]، فانه يمكن القول أن آلية عمل الانترنت و اختلاف مميزاتها و التي تكتنفها مصاعب جمة منها، صعوبة معرفة الطرف

---

[1] - ذياب موسى البداينة ،"الارهاب المعلوماتي "(2008)،اطلع علبه بتاريخ 06 ماي 2018

https://repository.nauss.edu.sa/bitstream/handle/123456789/56415/.pdf?sequence=1&isAllowed=y

[2] - كيستوتيس بولاوسكاس،"حول مفهوم الردع"،مجلة الناتو(2016)، اطلع عليه بتاريخ 18 أفريل 2018
https://www.nato.int/docu/review/2016/Also-in-2016/nato-deterrence-defence-alliance/AR/index.htm

المعتدي وصعوبة وضع الخصم موضع تهديد مع صعوبة منع الهجمات الصفرية[1] و التي تنتج عن التحديث المستمر للفضاء الرقمي و الاستغلال المستمر للثغرات بهدف انتاج فيروسات جديدة.

تتمثل أهمية الردع الرقمي في ضرورة التصدي لمختلف الطرق التي يحدث بها الاختراق الرقمي أو تشن بها الهجمات الرقمية و تتزايد أهميته في ظل هشاشة الدول و ضعف استجابتها لتلك الاختراقات، خاصة و أن الأمر يتطلب دمج كل عناصر السلطة الوطنية و الدبلوماسية والعسكرية و الاقتصادية و الاستخباراتية و القانونية بغية تعزيز الأمن المعلوماتي و خلق حالة في أذهان الأعداء حول فعالية أي نشاط رقمي مع زيادة تكلفته و عواقبه. وقد تعددت التعريفات المعنية بالردع الرقمي فمن جهة فهو يعني " منع الأعمال الضارة ضد الأصول الوطنية في الفضاء"ومن جهة ثانية يعني " خلق مجموعة المحفزات المناعة لمنع أحد أطراف الصراع من القيام بإعتداء أو هجوم مستقبلا"[2] مع العلم أنه لا يستطيع أحد الأطراف تدمير الطرف الآخر كليا، أما التعريف الأبرز و الذي سجل تداوله في الأوساط العلمية و الأكاديمية هو تعريف الجنرال أندريه بوفر الذي يرى بأن الردع الرقمي يعني "منع" دولة معادية من اتخاذ قرار باستخدام أسلحتها" أو بصورة أعم منعها من العمل او الرد ازاء موقف معين باتخاذ مجموعة من التدابير و الاجراءات التي تشكل تهديدا كافيا حيالها و النتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة بسيكولوجية نفسية. وبهذا فالردع الرقمي يقوم أساسا على خلق الحاجز النفسي لدى الخصم بما يضمن امتناعه عن الهجوم و التهديد مستقبلا.

ثانيا : ركائز الردع الرقمي

يرتكز الردع الالكتروني على ثلاث ركائز أساسية:

1- مصداقية الدفاع: تتطلب عملية ردع محاولات الاختراق توفر أنظمة نسخ احتياطية Backupsytems لتجنب الفقدان الكلي لمحتوى الأنظمة الأصلية في حالة تعرضها لهجوم ناجح،وتنبغي الاشارة إلى أن هذا الحل رغم تكلفته يعد عمليا أكثر و أكثر فعالية.
2- القدرة على الانتقام: تعني وجوب تكبيد المهاجم أضرارا تفوق ما وقع على المدافع منها ، وهو ما يتطلب القدرة أيضا على تنفيذ هجمات رقمية انتقامية كثيرة متتالية ضد المهاجم الأصلي ، ورغم أن هذاالأمر صعب التحقيق نوعا ما اذ أنه يستلزم التعرف على المهاجم أولا و قبل كل شيء.
3- الرغبة في الانتقام: أي أن إمتلاك القدرة على الانتقام لا تكفي بمفردها لردع المعتدين بل يجب على المدافع أو من تعرض للهجوم الاعلان صراحة عن رغبته في الانتقام من مهاجميه[3].

و هنا يجب توضيح أن مفهوم الردع يكتنفه الكثير من الجدل الذي انقسم إلى ثلاث اتجاهات : يرى الأول عدم جدوى نظرية الردع على صعيد الفضاء السيبراني أما الثاني فانه يؤكد على ضرورة تبني الردع السيبراني كجزء لا يتجزأ من استراتيجيات الأمن القومي للدول، فيما يذهب الاتجاه الثالث للإقرار بملائمة نظرية الردع للفضاء الرقمي بشرط وضع ضوابط محددة و التي منها

---

[1] - الصباحي ،" أبعاد القوة" ،**مرجع سابق. .**
[2] -البهي ، "الردع السيبراني "،مرجع سابق.
[3] -البهي،مرجع سابق

وجوب تبني مفهوم واسع للردع الرقمي[1] و المزج بين خيارات عدة في سبيل الوصول إلى استراتيجية متكاملة تدمج كل المقومات العسكرية و الاقتصادية و الاستخباراتية و القانونية أيضا.

وهو الاتجاه الذي يقودنا إلى التطرق إلى أهم الاشكاليات التي تواجه القادة في سعيهم لتطبيق الردع الرقمي.

ثالثا :اشكاليات تحقيق الردع الرقمي

الاسناد:[2]**:** يتطلب نجاح الردع الاعلان الرسمي للجناة عن مسؤوليتهم عن الهجوم و في غالب الأحيان يدعي ارهابيون المسؤولية عن هجوم ما في حين يفضل المهاجم الفعلي اخفاء مسؤوليته.

ان صعوبة تحديد مرتكب الهجمات بدقة قد تسفر عن استهداف طرف ثالث لا علاقة له بالهجوم ابتدءا ،مما يضعف من منطق الردع ويخلق معه عدوّاً جديدا، وتسعى الدول بغية تخطي هذه العقبة لاستخدام المصادر الاستخباراتية غير السيبرانية أي التقليدية Non-cyber intelligence للمساعدة في اكتشاف مرتكبي الهجوم في ظل استحالة اكتشافه من خلال الوسائل التقنية وحدها، فتحسين سبل الاسناد ضرورية لفعالية الردع وهو ما يستدعي تحسين القدرات على جميع الأصعدة كنقل الأدلة الرقمية و انشاء "خط انذار مبكر " و نقل للحرب السيبرانية يتيح الاختيار بين مجموعة كبيرة من أساليب الاستجابة السريعة.

-تجنب الانتقام أو الرد المضاد: صعوبة التنبؤ وبالتالي السيطرة على الهجمات السيبرانية يطيل المسافة الزمنية بين الهجوم و الرد، لذا فقد يبدو عند حدوثه ردا تعسفيا لا علاقة له بالحادث الأصلي، فضلا عن أن زيادة الأخطاء تستدعي أيضا الرد في مجالات أخرى مثل ما حدث عندما أعلنت، روسيا عام 1998 عن احتفاظها صراحة بخيار الرد على أي هجوم سيبراني باستعمال أي سلاح بما في ذلك أسلحتها النووية.

-العقوبات القانونية**:** لا يزال النقاش دائرا حول المسائل القانونية المتعلقة بالمجال السيبراني ففي ظل تحريم القانون الدولي للعدوان العسكري، قد يبدو الرد الانتقامي عملا عدوانيا غير مبررا أو مخالفا لقواعد القانون الدولي، فهل يحق للدولة الرد بالمثل في حالة التعدي عليها بهجوم رقمي أسفر عن تدمير قواعد عسكرية مثلا؟

- تدخل الفاعلين من غير الدول**: و**هو ما يضفي المزيد من التعقيد على مسألة تحقيق الردع السيبراني اذا يصعب استهداف الفاعلين فماذا أن كان المهاجم جماعة ارهابية أو منظمة غير حكومية تطلق هجماتها من دولة ما في حين تتمتع بالحماية من طرف دولة أخرى و هو الأمر الذي يطرح مرة أخرى مشكلة تحديد المواقع الجغرافية لمصادر التهديد و التي لا تعبر بالضرورة عن مصدر الخطر الحقيقي.

- ارسال رسائل صادقة واضحة للخصم: بدونها تزداد احتمالات سوء فهم الردع و تجاهله وهو ما يسهم في تصعيد الصراع فضمان عدم اساءة تفسير الاشارات يسمح باستعراض القدرات و النوايا ويتيح خيارات واسعة من الردع[1].

---

[1]- مرجع سابق.

ـ الوقت: احدى التحديات الرئيسية التي تواجهها نظرية الردع في الفضاء السيبراني هو القدرة على الكشف عن الهجوم في الوقت المناسب[2]، اذ لا يمكن مراقبة ورصد الهجمات السيبرانية قبل

وقوعها نظرا لطبيعة الأسلحة الرقمية في ظل امكانية تطوير القدرة الهجومية الرقمية دون توفر امكانات او اجراءات فعالة لردعها كما هو حال الأسلحة التقليدية أين يتم مراقبة نشاطات منصات الصواريخ و الغواصات باستمرار.

ـ نقص مصداقية كل من الردع بالانكار و العقاب: فالأول أي الردع بالحرمان غير وارد تماما بسبب يسر استخدام الوسائل التكنولوجية و سهولة توفرها وامتلاكها، وبما أن الردع بالعقاب يبقى الخيار الأوحد فأنه يظل يفتقر للمصداقية بسبب تغير حسابات الخصم أو عدوله عن العدوان.

المصداقية: كعامل رئيسي يبنى على ثقة المهاجم في قدرة الدولة على الانتقام و الرد، يتقوض ببساطة بما أن اختبار الأسلحة السيبرانية هو الدليل الوحيد على وجودها اذ لا يمكن للمهاجم معرفة ما اذا امتلك خصمه القدرة على الرد و الانتقام أو لا.

وختاما فان عدم القدرة على تحديد الأصول التي يمتلكها الخصوم و تعريضها للخطر المتكرر يشكل تحديا آخر تصاحبه اشكاليات ثانوية كاحتمال وقوع خسائر مضادة ،[3]ومجمل القول أن الاتساع الشديد للمجال خلافا لمجالات العسكرة الأخرى يتطلب بناء استراتيجيات فعالة بخصوص الردع الرقمي، اذ رغم فعاليته الجزئية خلافا للردع النووي فاستعماله أفضل من عدمه في شتى الأحوال.

رابعا: متطلبات الردع الرقمي:

يتطلب الردع الرقمي تطبيق أساليب و طرق جديدة و إعادة تكييف مفاهيم الردع التقليدية لتتناسب مع هذا المجال فلا يمكن معرفة الهدف من الهجمات دون تحديد مرتكبيها، أي الخصم في أوضح صورة ممكنة.

أ- الخيار الأول: الردع السلبي: و هو إجراء يستهدف تحسينا في تدابير الأمن السيبراني بما يرفع من تكاليف الهجوم الرقمي[4] مّما يؤدي إلى تقليل فرص حدوثه مستقبلا، ورغم اعتماده على عدم الرد على الخصم بالمثل و كونه أقل تعقيداً الا أنه يتسم بعدم الواقعية إذ يمكن للمهاجم أن يستخدم عدم الرد المباشر بالهجمات كفرصة لمواصلة الأنشطة العدائية الرقمية على نحو أوسع و هوالاعتقادالذي تتبناه الولايات المتحدة بأن الرد عن طريق الانكار هو استراتيجية سلبية.

ب- الخيار الثاني: الاحتجاجات الدبلوماسية: رغم عدم تسببه في الأضرار الكافية التي تردع الدولة المهاجمة عن شن هجمات مستقبلية الا أنه يضر بسمعتها على الصعيد الدولي و يتمثل هذا الخيار في طرد مسؤولي الدولة التي يشتبه أن لها ضلعا في شن الهجوم السيبراني.

---

[1] -البهي ،"الردع السيبراني"،مرجع سابق

1-الصباحي،"أبعاد القوة"، مرجع سابق.

[3] -البهي ، " الردع السيبراني"،مرجع سابق

[4] - Emilio IasiEllo , " La cyber-dissuasion est-elle une stratégie illusoire ?", ASPJ Afrique & Francophonie , 1er trimestre(2018), 42
http://www.airuniversity.af.mil/Portals/10/ASPJ_French/journals_F/Volume-09_Issue-1/iasiello_f.pdf

ج- الخيار الثاث: التدابير القانونية**:** شأنها شأن الاحتجاجات الدبلوماسية تتخذ طبيعة رمزية في غالب الأحيان كاقامة دعاوى قضائية مّما يهدد بكشف معلومات استخباراتية حساسة، الا أن هذا الخيار يمكن أن يتسبب في اضرار اكثر مّما يستحق الأمر و هو ما يخفف من تأثيره الردعي.

د-الخيار الرابع**:** وهو الأسلوب الذي تنتهجه الولايات المتحدة الأمريكية و المتمثل في تعزيز العقوبات الاقتصادية على الدول المشتبهه قيامها بالعدوان السيبراني ككوريا الشمالية وعدوانها على شركة سوني بيكتشرز، ورغم فعالية هذا الخيار الا أن تداعياته المحتملة كبيرة حتى على الدول التي تقوم بفرض العقوبات بسبب اضراره بمبادئ الاعتماد المتبادل بحكم ارتباط اقتصاديات الدول بعضها ببعض و تداخل المصالح و تشابكها دوليا في ظل غياب مبادئ توجيهية حول كيفية التخفيف أو التخلص من العقوبات لاحقا فيظل عندئذ تغيير الدولة لسلوكها غير مبرر و بالتالي غير مقبول[1].

ه)الخيار الخامس:الانتقام في الفضاء الافتراضي: و يعد سببا من أسباب التصعيد المتبادل و مظهرا من مظاهر سباق التسلح السيبراني فالتهديد بالانتقام شكل دوما رادعا فعالا ازاء الهجمات السيبرانية المستقبلية المتمثلة في استهداف البنية التحتية للخصم و سرقة المعلومات الخاصة به و نشر الأنباء الكاذبة عنه و هو ما يجعله خيارا فعالا.

و) الخيار السادس: الانتقام العسكري: عدم واقعية هذا السبيل الرادع نابعة من كونه يعد شرارة بدء عملية تصعيد خطير اذا يسفر استخدامه عن رد عسكري مضاد حتما[2]، ورغم احتمالات وروده الكبيرة خاصة اذا ما نتجت عن الهجمات السيبرانية خسائر كارثية تستدعي اعادة تعديل فورية لموازين القوى، الا أنه يظل يصطدم بمعظلتي سرعة الرد[3] و اشكالية الاسناد و التي تهدد بجعل الضربة المضادة آلية للرد و الدفاع و ليس للردع.

و بالرغم من أن هذا الخيار يعكس تهاوي مصداقية الردع السيبراني بحكم اللجوء للقوة العسكرية للرد على هجومات تطال المجال الرقمي أساسا نظرا لحجم الأضرار التي يستلزم احيانا ردا سريعا و حاسما.

الا أنه يظل خيارا قائما بسبب الاختلافات الجوهرية التي تساهم في تشكيل الردع في عصر التطور المعلوماتي عنه في عصر الحرب الباردة.

وتحاول الدول جاهدة التغلب على مجمل هذه المصاعب باعتماد اقترابات مختلفة تم تداولها بشكلين اثنين:

1-**الأنظمة البديلة:** درءا للعواقب التي غالبا ما تنجر عن اعتماد نظام واحد، يمكن الاستعانة بالأنظمة الاحتياطية التي تكون في حوزة الدولة أو لدى الدول الصديقة.

---

[1] -رغدة البهي، " الردع السيبراني"،مرجع سابق

[2] - نسرين فوزي اللواتي ،"الردع الالكتروني :العامل الحاسم في مواجهة الخصوم "،لغة العصر(2017)،آخر تحديث 25 ماي http://aitmag.ahram.org.eg/News/77865.aspx2017

[3] -Ibid, Emilio IasiEllo, " La cyber-dissuasion" , 41

2-اعادة التأسيس: القدرة على التغلب على الهجوم و اعادة النظام تحول الآثار المتوخاة من الردع إلى آثار هامشية لا تذكر و تظل مسألة الاحتجاب عن الجميع أفضل السبل لتحقيق الردع السيبراني.[1]

رغم ما يكتنفها من مسائل قانونية عدة.

كما أن استراتيجية الردع الفعالة يجب أن تعتمد على أنظمة مرنة تمكنها من التعافي سريعا من الهجمات فبالاظافة إلى نشر دفاعات قوية ينبغي اتخاذ الوسائل اللازمة على نحو يتسق مع قواعد القانون الدولي للرد على الهجمات العكسية الدفاعية و الهجومية بشكل يستنفذ جميع الخيارات المتاحة لاستخدام القوة العسكرية.[2]

و تتطلع الدول في هذا الشأن لانشاء قوات متخصصة في الردع السيبراني في محاولة منها للتصدي للهجمات الفعلية و المحتملة مع شحذ تقنيات الاستخبارات لاكتشاف هوية المهاجمين بغية تشديد الاجراءات القانونية الرادعة التي تضمن أمن و فعالية شبكة الإتصالات الدولية و هي المسألة التي لم تمنعها من الاعتماد على اظهار قدراتها التقليدية في عملية استعراض قدرات الاستجابة[3].

تحديات الردع الرقمي:

من شأن الردع السيبراني الفشل طالما لم يعلن الجاني رسميا عن مسؤوليته عن الهجوم فمن الممكن أن يدعي إرهابيون مثلا مسؤوليتهم عن الهجوم فيما لا يرغب المهاجم الفعلي في الإعلان عن نفسه يمكن حينئذ لأي شخص أن يكون الجاني خاصة وأنه في الهجمات السيبرانية يمكن الوصول للمعدات لشن الهجومات الرقمية بيسر كما أنها ليست مكلفة و يمكن شنها من أي مكان تتوفر فيه خدمة الانترنت .

و لكي يعمل الردع بصفة فعالة يجب أن يقلق المهاجم من كشف هويته ومن ثم تعرضه للعقاب أو الانتقام ،كما أن صعوبة تحديد مرتكب الهجمات بدقة قد يسفر عن استهداف طرف ثالث لاعلاقة له بالهجوم الأول ابتداءا.وهو الأمر الذي لا يضعف فقط من منطق الردع وفلسفته ولكنه يخلق عدوا جديدا أيضا .

فمن الصعب جدا وغالبا ما يكون مستحيلا اسناد الهجوم السيبراني الى مرتكبيه بمجرد اكتشافه[4].

المطلب الثاني : الدفاع الرقمي

---

[1] - البهي ،" الردع السيبراني"،مرجع سابق

[2] -Ibid, Emilio IasiEllo, " La cyber-dissuasion" ,47

[3] - البهي، " الردع السيبراني"، مرجع سابق

[4] - ايهاب خليفة ،"cyber pawer: التطبيقات الأمنية لقوة الفضاء الالكتروني"،المركز العربي لأبحاث الفضاء الالكتروني(2014)،آخر تحديث 16 سبتمبر 201
http://www.accronline.com/article_detail.aspx?id=19817

يشكل مصطلح الدفاع الرقمي مصطلحا حديثا جرى تداوله بكثرة مؤخرا في الاوساط السياسية و العسكرية و الامنية مشيرا بذلك للوعي المتنامي من طرف الدول و الحكومات لحجم الضرر الذي باتت تسببه التطبيقات العسكرية للفضاء الرقمي.

أولا: سياسات الدفاع الرقمي:

اعلنت 130 دولة حول العالم عن قيامها بتخصيص أقسام للأمن السيبراني و انشاء هيئات للدفاع الرقمي بهدف حماية الشبكات و أنظمة تقنية المعلومات التشغيلية سواء كانت أجهزة أم برمجيات[1]. و بغية فهم أفضل لأنظمة الدفاع العسكري تجدر الاشارة الى أن أجهزة السيطرة على الصواريخ و البنوك و غيرها من أجهزة الأمن القومي كلها مرتبطة بشبكات و هذه الشبكات تستخدم كلها الانترنت[2]، وبغض النظر عما توصلت إليه التكنولوجيا في حماية هذه الشبكات فان أي عملية اختراق أو اكتشاف ثغرة صغيرة داخل نظام عملها تسمح بزرع فيروس داخلها مما يؤدي التي تعطيل عمل هذه الأنظمة أو التسبب في حدوث عمليات إعطاء أوامر عكسية كإطلاق الصواريخ الحاملة للرؤوس النووية و ما إلى ذلك من الأضرار التي لا يمكن توقع آثارها المدمرة فإطلاق صاروخ واحد يمكن أن يكلف دولة كبرى كالولايات المتحدة الأمريكية سنوات من الاصلاح فضلا عن ردود الفعل الدولية غير المرغوب فيها خاصة وأنه لا يمكن اكتشاف الفيروس الذي يستخدم التكنولوجيا الحديثة إذا كانت تكنولوجيا لم يتم اكتشافها بعد الا بعد حدوث الضرر، فلا توجد شبكة محمية 100% و لايوجد هناك نظام خال من الثغرات حتى مايكروسوفت نفسها تصارع من اجل البقاء و لديها فريق من أشهر الهاكرز و الكراكرز لسد ثغرات الوندوز.

بغرض مواجهة هذه التحديات تسعى الدول لإدخال الفضاء الرقمي ضمن استراتيجياتها للأمن القومي و إتباع سياسات دفاعية مختلفة تنوعت بين:

- تحديث الجيوش و تدشين وحدات متخصصة في إدارة الحروب السيبرانية.
- إقامة هيئات وطنية للأمن و الدفاع الرقمي.
- القيام بالتدريب و إجراء المناورات لتعزيز الدفاعات الألكترونية.
- العمل على تعزيز التعاون الدولي ومجالات تأمين الفضاء الرقمي.
- القيام بمشروعات وطنية للأمن الألكتروني.
- تبنى الدول إستراتيجية حرب المعلومات باعتبارها حرب المستقبل التي يتم خوضها بهدف التشتيتت و إثارة الاضطراب.[3]
- جذب الكوادر الوطنية المؤهلة و الطموحة و القيام بتأهيلها في مجال الدفاع الرقمي.
- تحفيز الابتكار و الاستثمار في مجال الدفاع الرقمي و الأمن السيبراني.
- بناء الشراكات مع الجهات العامة و الخاصة المهتمة بالحفاظ على الأمن القومي.
- تحديث و حماية أنظمة التوجيه للقطارات و الطائرات و الأنظمة المصرفية.

---

[1] -عبير محمد ،"الامن السيبراني"،المرسال (2017) ،اطلع عليه 18 أفريل 2018
https://www.almrsal..com/post/552008

[2] -"مخاوف أمريكية من هجمات الكترونية"،الجزيرة ، على الرابط www.ahjazira.net/programmes/ اطلع عليه بتاريخ 12 افريل 2018

[3] -عباس بدران ،" الحرب الالكترونية :الاشتباك في عالم المعلومات"،مركز دراسات الحكومة الالكترونية (لبنان :بيروت ،الطبعة الأولى ،2010)،05

و هذا كله يستدعي وضع خطط عمل وطنية واسعة النطاق لإعادة هيكلة الشبكات الحاسوبية و المصرفية و التجارية و الطاقوية و النقل لتوفير إمكانية التعامل مع الهجمات الرقمية المهمة و الهائلة و المرتقبة.[1]

ثانيا:الجيوش الرقمية:

الجيش الرقمي هو مجموعة من الأشخاص و قراصنة الأنترنت الهاكرز و الكراكز تعمل لصالح المخابرات و الأمن في الدولة، وقد انتشر المصطلح بشكل كبير عام 2011 عقب الكشف عن الجيش الالكتروني السوري الذي نجح في اختراق مواقع أوربية و أمريكية و عربية [2]. وتحول سعي الجيوش الحديثة أو " الذكية " لانجاز مهامها بصور الأقمار الصناعية و الأجهزة التي تلتقط الصور حتى من ساحة المعركة إذ لم يعد الجهد و لا الزمن عائقا أمامها، فتلقي الأوامر من الزعماء السياسيين و العسكريين صار يتم عبر الأجهزة المتطورة التي تضمن أمن و سلامة محتويات وحدات أخرى، أضحى الهدف من تشكيل وحدات الرقمية متخصصة هو المساعدة على خلق عوامل النجاح المتمثل في جيوش رقمية كاملة تنقل ساحة المعركة من الواقع الفعلي إلى الواقع الافتراضي في خطوة جريئة.

وتعد ظاهرة تأسيس الجيوش السيبرانية بداية سياسات دفاعية جديدة هدفها إدارة العمليات المتقدمة في مجال الفضاء السيبراني و تعمد الجيوش لتأسيس غرف حرب رقمية digital warroom والتي تعتبرها الدول مركز أعصاب الدولة في عمليات الحماية حيث يكون بمقدورها القيام بعمليات اعتراض و توجيه و تشغيل في الفضاء الرقمي بالتنسيق مع جميع وحدات الجيش[3].

حيث يحرص الجيش على مشاركة مندوبين من شعبة الاستخبارات العسكرية و شعب المعالجة، و تختص بعض وحداته في الاعداد للبرامج المستقبلية لتحسين جاهزية العمل في مجال الدفاع السيبراني.

ثالثا :معايير امتلاك القدرة الالكترونية:

-اعتماد نظام تعليمي متقدم يدمج مجالات البرمجة و الذكاء الصناعي في مناهج التدريس الأساسية.

-تحديد أهداف الدولة الإستراتيجية ضمن خطة إستراتيجية محكمة تعظم القدرة الالكترونية.

-حيازة بنية سيبيرانية cyber infrastructure [4]تقدم خدمات الكترونية متنوعة للشعب.

---

[1] -ايهاب خليفة،"القوة الالكترونية "،مرجع سابق

[2] -" الجيش السوري الالكتروني"،موسوعة ويكيبيديا(2018)،آخر تحديث 29 جانفي 2018
https://ar.wikipedia.org/wikiالجيش_السوري_الإلكتروني

[3] - كمال مساعد ،"الحرب الرقمية ومنظومة السيطرة الكاملة"، مجلة الجيش(2003)،آخر تحديث جويلية2003
https://www.lebarmy.gov.lb/ar/content/الحرب-الرقمية-ومنظومة-السيطرة-الكاملة

[4] - ايهاب خليفة ،" القوة الالكترونية" ، مرجع سابق

-تطبيق إجراءات تأمينية صارمة و فعالة بوسعها التصدي للهجمات الرقمية.

-تدريب عناصر بشرية موثوق في ولاءها لامتلاك المعرفة التكنولوجية الحديثة و استخدامها بمهارة فائقة.

توفير أجهزة مختصة بالدفاع السيبراني تقوم بالتنسيق مع الجهات الأمنية كالشرطة و غيرها بغرض التحقيق في الجرائم الالكترونية و تكون تابعة للقوات المسلحة الوطنية.

-امتلاك الدولة للقدرات الهجومية السيبرانية التي تمكنها من مهاجمة شبكات الحاسب الآلي للعدو عند الضرورة سواء بغرض الردع أو بغرض استطلاع الشبكات الأخرى مع القدرة على الدفاع عن شبكاتها الخاصة[1]

جدول يوضح القدرات الالكترونية لبعض الدول[2]:

الدولة	الهجوم الالكتروني	الاعتماد على الفضاء الالكتروني	الدفاع الالكتروني	المجموع
الو م أ	8	2	1	11
روسيا	7	5	4	16
الصين	5	4	6	15
إيران	4	5	3	12
كوريا الشمالية	2	9	7	18

المصدر : **نوران شفيق ،" أثر التهديدات الالكترونية على العلاقات الدولية :دراسة في أبعاد الأمن الالكتروني " جامعة القاهرة (2014)**

شفيق ، نوران. "أشكال التهديدات الالكترونية و مصادرها ". المركز الأوروبي لدراسة مكافحة الارهاب و الاستخبارات(2017) .آخر تحديث 10 ديسمبر 2017.
https://www.europarabct.com/B1%D9%87

المطلب الثالث: الجهود الدولية و اشكالية الحد من التسلح الرقمي

1- **التشريعات الحكومية :**

---

[1] - إيهاب خليفة ،"عناصر القوة الالكترونية"،مرجع سابق

[2] - **نوران شفيق ،" أثر التهديدات الالكترونية على العلاقات الدولية :دراسة في أبعاد الأمن الالكتروني "، جامعة القاهرة (2014)،41**

لقد عمدت عدة حكومات لتبني تشريعات قانونية من أجل الحد من التسلح الرقمي، فالتشريعات الأمريكية وبناء على جهود الكونغرس صدر قانون جرائم الحاسب الآلي سنة 1984 تحت مسمى قانون الاحتيال و اساءة استخدام الحاسب الآلي The computer frond and abuse act و الذي تم تمديده مرتين الأولى عام 1986 و الثانية سنة 1994 و يعتبر بموجبه الوصول الى المعلومات الحكومية المصنفة بدون رخصة من عداد الجنايات . أما المملكة المتحدة فقد أصدرت التشريع البريطاني في 29 جوان 1990 تحت اسم "قانون اساءة استخدام الكمبيوتر ، يتم بموجبه تجريم الحصول على مواد غير مصرح بها من كمبيوتر معين " . في حين أصدر التشريع الفرنسي قانون العقوبات لسنة 1998 يُجرم الدخول لنظام المعالجة الآلية للمعلومات أو البقاء فيها بطريقة غير مشروعة . كما وقد سجل اهتمام السعودية التي احتلت المركز السادس عالميا للدول التي تنطلق منها الهجمات لاصدار مرسوم ملكي تنظم بموجبه آليات مجابهة الظاهرة .[1]

و يختلف التصدي للجرائم المعلوماتية من دولة الى أخرى، ففي حين تعمد الدول لاقرار تشريعات خاصة بها ،تلجأ أخرى للانتربول لعدم توفرها على أجهزة متخصصة في أمن المعلومات وعدم حيازتها لاطار مؤسسي تشريعي منظم لمكافحة الظاهرة .

ثانيا: تشريعات المنظمات الدولية: نذكر منها القرارات والإتفاقيات الصادرة عن المنظمات الدولية ومنها:

1- الأمم المتحدة : أصدرت الجمعية العامة قرارا في 1990/12/14 .
2- منظمة التجارة العالمية : عقدت اتفاقية تنظيم و انتقال المعلومة يوم 1994/04/15 والتي أكدت فيها على حرية انتقال المعلومات بين الدول دون تمييز أو اتخاده كذريعة خفية للحظر التجاري ولا يمكن تفسير أي تدبير وارد في هذا الاتفاق كسبب لامتناع أي عضو من تطبيق ما ورد فيه .
3- منظمة العمل الدولية : بذلت جهدا كبيرا في مجال حماية المعلومة الشخصية المتعلقة بالعمل،و في تقنينها لمجموعة توصيات للعملية التي تباناها مكتب العمل الدولي[2] خلال مؤتمر الخبراءالذي أقيم في جينيف عام 1996 .
4- المجلس الأوروبي : له دور بارز في محاولة تنظيم نشاطات الفضاء الرقمي و من أهم أعماله: اتفاقية بوداباست : عرفت فيها بعض المفاهيم المتعلقة بنظام الكمبيوتر و الخدمات و تعتبر هذه الاتفاقية ملزمة للدول الموقعة عليها في 23 نوفمبر 2001 و المتعلقة بالاجرام الكوني أي الاجرام المعلوماتي الذي حول من استخدام الفضاء المعلوماتي لأغراض غير شرعية، و عملا على تطبيق السلطات للاجراءات المقررة في بيئة تكنلوجيا المعلومات، حرص مجلس أوروبا للتصدي للاستخدام غير الشرعي للحسابات و الشبكات و المعلومات في صياغة اتفاقية شاملة.[3]

---

[1] - محروس نصار غايب ،"الجريمة المعلوماتية"،"،المعهد التقني الأنبار(2011)13و14و15و16، اطلع عليه بتاريخ05 ماي 2018 https://www.iasj.net/iasj?func=fulltext&aId=28397

1-محمود نصار غايب ،"الجريمة المعلوماتية"،مرجع سابق

2- العربي ،محمد مسعد ."من الدولة الى الفرد : تأثير السياسات الافتراضية الصاعدة في العلاقات الدولية ". السياسة الدولية(2013).آخر تحديث20 نوفمبر 2013.

- http://www.siyassa.org.eg/News/3352.aspx

ثالثا- الجهود الدولية:

يقول شرستيوك " بما أن الحديث يدور حول أمن البشرية جمعاء لذلك فان حل هذه المشكلة ممكن فقط بتعاون الجميع "[1]. تم طرح مسألة تهديد العسكرة الرقمية للأمن الدولي و الوطني في العديد من المؤتمرات و المنتديات الدولية حيث أوضحت الأطراف المشاركة ضرورة شراكة الدولة و القطاع الخاص و المجتمع المدني في ضمان الأمن المعلوماتي.

و لقد كانت روسيا من أوائل الدول التي دعت لتأطير إستخدامات الفضاء الرقمي ووضع قيود على تطبيقات استخداماته العسكرية، حيث انعقد بموسكو مؤتمر شارك فيه 100 مائة خبير مثلوا 12 بلداً،ناقشوا فيه طرق و أساليب تنظيم وتأطير استعمالات الفضاء السيبراني .

غير أن عمل الخبراء لم يكن له الوزن المطلوب فالدول بحاجة لاتفاقات دولية مقبولة يمكن تنفيذها و الالتزام بها.وهو الأمر الذي لا يزال بعيدا عن متناول الخبراء اذ يدخل في صلاحيات القادة و صناع القرار و الذين يفتقرون للمعرفة التكنلوجية اللازمة التي تخولهم ادراك حجم التحديات التي باتت تهدد أمن و سلامة الدول.[2]

غير أن تصاعد الاحتجاجات في البلدان الديمقراطية كالولايات المتحدة و بريطانيا[3]، دفع بعدد من الدول الكبرى كالولايات المتحدة الأمريكية لعقد مناقشات ثنائية مع روسيا أظهرت استعدادا بين الأطراف المتنازعة لتسوية القضايا المتعلقة باستخدام التكنولوجيات الالكترونية في المجال العسكري.

لكن الملاحظ أن الجهود الحادة التي انصبت لدراسة الأخطار الرقمية و محاولات ايجاد آليات قانونية للحماية منها و التي قادتها المنظمات و الهيئات الدولية الاقليمية خاصة الأوروبية منها، جاءت أساسا تداركا لقصور القوانين الجنائية الخالية من النصوص المحيطة بالجرائم الرقمية بسبب صعوبة تصنيفها، مما استوجب وضع قوانين و تشريعات خاصة بالمسألة.

و على المستوى المحلي قامت البلدان باستحداث أقسام خاصة بالتحقيق الفني تعمل على تقديم الدعم التقني لجميع أقسام البحث الجنائي الأخرى، ويعتبر الاقتراح الروسي عام 1999 لاقرار معاهدة في اطار الامم المتحدة تهدف لحظر استعمال الأسلحة الالكترونية و المعلوماتية[4] بما في ذلك الدعاية المغرضة اللبنة الأولى في هرم التعاون الدولي المشترك لمكافحة سوء استخدام الفضاء الرقمي.

كما سجل سعي الصين و غيرها من أعضاء منظمة شنغهاي للتعاون لضمان استمرار هذه المعاهدة بغية الوصول الى اتفاقية أممية عامة، لكن هذه المحاولات فشلت بسبب مقاومة الولايات المتحدة الامريكية لها اذ اعتبرتها محاولة للحد من قدراتها الالكترونية وبدلا من ذلك اتفقت مع روسيا و 13 دولة اخرى سنة 2004 على أن يعين الأمين العام للأمم المتحدة الأمريكية مجموعة

---

[1] -"السلاح السيبراني أخطر من النووي"، صحيفة ايزفيستيا(2016) ،آخر تحديث29 أفريل2016
https://arabic.rt.com/press/821142السلاح-السيبراني-النووي-

[22] - أحمد عبيس الفتلاوي،"الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر (العراق:جامعة بابل ،2015)، اطلع عليه بتاريخ 12أفريل 2018

[3] -عبد الصادق،"الفضاء الالكتروني و أسلحة الانتشار الشامل" ، مرجع سابق

[4] -جوزيف س ناي الابن،" التحكم في الصراع السيبراني"، مدونات الجزيرة(2017)، 09 أوت 2017
http://blogs.aljazeera.net/blogs/2017/8/9

من الخبراء الحكوميين بيد أن الاجتماع لم يسفر الا عن نتائج هزيلة و استمرت الجهود متواصلة حتى جويلية 2015 اين أصدرت تقريرا أقرته مجموعة العشرين يقضي بوضع معايير مقترحة للحد من تدابير الثقة، غير أن كل هذه الجهود واصلت في التعثر فقد فشلت في اصدار تقرير بتوافق الآراء عام 2017 بسبب الحدود التي أعاقت تقدم عمل فريق الخبراء الحكوميين بسبب فقدانهم للصلاحيات الكاملة التي يحوزها المفاوضون الوطنيون.

ورغم بوادر الأمل التي لاحت اثر اعراب سبعون دولة عن الرغبة في المشاركة في عمل المجموعة، الا أن هذا لم يزد الا من تقهقر النجاحات بسبب صعوبة التوصل الى اتفاق يرضي كافة الاطراف.

ويبدو أن الوتيرة المتباطئة التي تسير بها الاجراءات المتخذة في هذا الصدد مردها الاعتقاد بأن القانون الدولي القائم حاليا ينطبق على الفضاء الرقمي و لا حاجة لاعداد اطار قانوني جديد بل يكفي اعتماد مبادئ للسلوك بين الدول اعتمادا طوعيا و اعداد تدابير من شأنها تعزيز الثقة بين الدول، و هذا هو الموقف الذي يمثل وجهة النظر الأوربية خاصة[1]، وهو ما يتجلى واضحا في سياسات الدفاع الرقمية المرسومة لدى الاتحاد الاوربي و منظمة حلف شمال الأطلسي.

4-معوقات نجاح الاتفاقات الدولية

يمكن حصر المعوقات التي واجهت نجاح الجهود الدولية لتأسيس الفضاء الرقمي و الحد من العسكرة الرقمية في:

1-الاختلافات في تحديد جهة السيادة في الفضاء الالكتروني و صياغة مفهوم العدوان الالكتروني[2].

2-اختلاف جمع المعلومات الاعتيادي عن الاعداد لعمليات تخريب الكترونية كما لم يتم التوصل الى صيغة موحدة لتصنيف السلاح السيبراني.

ويستقر الخلاف حول مدى صلاحية استخدام مواد القانون الدولي في تحديد مفهوم النزاعات العسكرية و الرد على العدوان اذا يرى البعض انها تسمح بمراقبة هذا السلاح الجديد اما البعض اللآخر فيطالبون بمنح استخدام هذا السلاح منعا باتا.

-الصعوبات التقنية الكبيرة التي تظهر عند تقييم العدوان الرقمي لاستحالة تحديد بلد المنشأ رغم ان مشكلة تحديد الهوية لم تعد معقدة كما كانت حتى قبل.

و لا تزال القوانين الوطنية و الدولية تعاني من اشكالية تحديد المعاملة القاتنونية الواضحة و هو الوضع الذي فرضته مميزات البيئة الرقمية فعدم امكانية اسناد الفعل الى مرتكبيه و صعوبة وضع معايير محددة للتعامل مع الجرم الرقمي بسبب ضعف الثقافة العدلية الرقمية عقد كثيرا من القضايا وهو الامر الذي ينبؤ عن عجز الدولة لوحدها في مواجهة هذا النوع من التهديد الذي يتطلب ايجاد منظمة قانونية دولية تعمل تحت مظلة الامم المتحدة.

---

[1] - غايب ، مرجع سابق.

[2] - فريق الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية، "دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير الي تتخذها الدول الاعضاء و المجتمع الدولي والقطاع الخاص للتصدي لها "، UNODC (23 جانفي 2013)، 14و15و16،اطلع عليه28 أفريل2018 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_A.pdf

من جهة أخرى:

فإن حالات الارباك لدى جهات انفاذ القانون تعكس المواقف المتناقضة التي تتها الدول بشأن تعزيز امن الفضاء الرقمي فبعضها يعتقد انه يجدر اعداد صك قانوني دولي ملزم يؤطر التدابير التي تتخذها الدول بينما تعتقد الاخرى انه و بحكم ان الدول ليست بالجهات الفاعلة المعنية الوحيدة فيجب العمل بشراكة مع المنشآت و المجتمع المدني [1]من أجل اعداد حلول ترمي الى تعزيز أمن الفضاء الرقمي و الحد من عسكرته مع ان شكل الدول تخشى من ان تؤدي مراقبة الفضاء السيبراني الى الحد من الحرية التي تستمر بها الانترنت.

وفي انتظار المتوصل لاتفاق يرضى الطموحات الامنية للدول الفواعل الدولية المختلفة لتعزيز وعي مراقبي البيانات، وتفعيل آليات الشكاوي القضائية ووضع مبادئ توجيهية دولية لتحديد القانون الواجب النفاذ حال التعارض بين القوانين.

وهو ما يتلزم الاخذ بالحسبان السرعة المطلوب لاجراء تحقيق جنائي او وطني بحكم التزايد حجم البيانات الذي يخلق تحديات جديدة كل يوم و يتطلب الاستثمار في الاشخاص ذوي المعارف و المهارات و استخدام التكنولوجيا الرقمية و تحليل البيانات مع أنه لا يوجد حل تقني أو قانوني واحد يمكنه التغلب على التحديات من قبل الجرائم المنظمة و الاختراق البيانات و التدفقات المالية غير المشروعة[2]

4- التسلح الرقمي و اشكالية الحد من التسلح

على الرغم من قدرة الحرب عبر الفضاء الرقمي على احداث ذات الضرر الناتج عن استخدام الاسلحة التقليدية الا ان مسألة الحد من التسلح الالكتروني أو السيبراني تواجهها مشاكل عويصة:

أولا: صعوبة فرض خطرا استخدام الاسلحة الرقمية في الفضاء الرقمي.

ثانيا:صعوبة وصف العمل على أنه هجوم مسلح وهي المشكلة التي واجهت موقف حلف الناتو عند الهجوم على استونيا.

ثالثا: عدم قدرة المجتمع المجتمع الدولي على التدخل لاحتواء التطور و التقدم في مجال السلاح بسبب عدم امكانية تحديد الاسلحة التي تمتلكها الاطراف الدولية.

رابعا: عدم وجود مجال لتفعيل التفتيش كآلية مراقبة مثل حالة الاسلحة النووية.

خامسا:الطابع الفردي و البشري الذي تستم به العملية[3]

تطوير القدرات في الحرب الالكترونية عامل مهم يساهم في الحد من امكانية احتوائها.

---

[1] -غايب ،مرجع سابق

[2] - رغدة البهي،" مخاطر سباق التسلح المعلوماتي في القرن الحادي و العشرين "، طومون رويترز و المجلس الاطلسي، FUTURE(01)2017(01نوفمبر 2017
https://futureuae.com/book.php/Mainpage/Item/3400/big-data

2-مرجع سابق

ورغم كل هذه الصعوبات فقد نجحت فرنسا في ادراج موضوع التطبيقات العسكرية للانترنت لاول مرة على جدول اعمال مؤتمر قمة مجموعة الثماني في دفيل في ماي 2011 [1]في محاولة منها لاقناع شركائها بضرورة التعاون من اجل تطوير الانترنت تطويرا متناسقا و ضمان الاستخدام السلمي للشبكة العنكبوتية " بما يخدم الانسان و الديمقراطية و النمو الاقتصادي "كما يسجل عمل وزارتها الخارجسة على المسؤولين الاوربيي و الدولي من اجل الترويج لفضاء رقمي آمن يحترم الحقوق الاساسية ويصب في خدمة التنمية و تجري مسألة معالجة أمن الفضاء الرقمي على مستويين إثنين:

1- مكافحة استعمال الفضاء الرقمي للأغراض الاجرامية.
2- حماية الفضاء السيبيراني من الاستهلاكات التي تمس بحسن سير أنظمة المعلومات و الاتصالات.

وتعتبر الجهود الفرنسية استكمالا للتدابير الخاصة بأمن الفضاء السيبراني، و التي أقرت في اتفاقية مجلس أوروبا الخاصة بأمن الفضاء الرقمي و التي وقعت في بودابست عام 2004 و التي تتضمن التعاون في مجال القانوني لمكافحة الجرم المعلوماتي[2].

- الجرائم التي تستهدف السرية.
- سلامة البيانات و النظم المعلوماتية و توفيرها للاستعمال.
- انتهاكات حقوق الملكية الفردية.

وهناك نزوع اووبي شديد لتحديد معايير للسلوك في الفضاء الرقمي مرده الاستهداف المتواصل للمنشآت الحيوية الأوروبية.

لذا فهي تؤيد أي اجراء كفيل بتحسين حماية البنى التحتية الحساسة للمعلومات على المستويين الوطني و الدولي.[3]

---

[1]- مرجع سابق

[2] - لموسخ محمد،" تنازع الاختصاصات في الجرائم الالكترونية"، محاضرة(ورقلة ،جامعة قاصدي مرباح ،قسم الحقوق) ،154
https://dspace.univ-ouargla.dz/jspui/bitstream/123456789/7143/3/D0211.pdf

[3]- غايب ،"الجريمة المعلوماتية "،مرجع سابق

الفصل الثالث :التنافس الرقمي الروسي الامريكي

المبحث الاول :العسكرة الرقمية الروسية

المطلب الأول: السياسية السيبرانية الروسية:

أولا: العقيدة الرقمية الروسية:

تنظر روسيا للانترنت بشكل مختلف تماما عن نظيرتها الغربية كما يعمل الانترنت كجزء من جهد كامل جنبا إلى جنب مع غيره من الأسلحة في الحرب.و يتخذ الروس من العسكرة الرقمية آلية لتمكين الدولة من السيطرة على المعلومات و المناظر الطبيعية التي تعتبر مجالا للحرب بحد ذاتها.[1]

وتدمج العقيدة العسكرية الروسية عمليات التضليل والتخريب السياسي ضمن أدوات الحرب الضرورية و بهذا يتحول التهديد الرقمي و الحرب السيبرانية لأدوات شرعية يحق للدولة إستعمالها في وقت السلم كما في زمن الحرب فتقليل القدرة للعدو أصبح متاحا بعد أن ساهمت غزارة المعلومات و تدفقها اللامتناهي من إفساح المجال للحصول على إمكانات واسعة و غير متناقضة تسمح بالتأثير على هياكل الدولة و السكان[2] .

و تجلى ميل روسيا نحو طمس الخطوط بين دول الحرب و السلام بعد أن غدت الحرب غير معلنة في إستخدام المعلومات بغرض تفكيك الحكومة واستغلال التنظيمات المناهضة للحكومة في تغذية الاحتجاجات و التأثير على الرأي العام و ردع الأعداء و الحد من إرادة الخصم.

و رغم أن الجيش الروسي كان بطيئا نسبيا بإعتناق السيبرانية لأسباب بنيوية عقائدية[3] إلا أن الكرملين أدرك بعد إعلان حالة الطوارئ في جورجيا أنه يجب إستخدام الانترنت كوسيلة "تمكين"اذ تعمد روسيا لتوظيف مقاربة مفادها توظيف الهجوم السيبراني كوسيلة لردع الخصوم متخذة مواقف أكثر حزما من قبل و مولية للتجسس الرقمي و التسلل الإلكتروني و الحرب النفسية مزايا إستثنائية.

أعلنت روسيا سنة 2010 عن عقيدتها العسكرية الخاصة و التي تشير إلى وجوب الإستخدام المتكامل للقدرات العسكرية و غير العسكرية في الصراعات الحديثة فعلاوة عن الإدارة السيبرانية داخل الجيش الروسي تم تشكيل قيادة مستقلة للأمن السيبراني لتعزيز جاهزية القوات المسلحة الروسية.و تعد روسيا من أوائل الدول التي سعت لعسكرة الفضاء الرقمي معطية أهمية خاصة لشبكات التواصل الإجتماعي.

ثانيا: الإستراتيجية السيرانية الروسية:

---

[1] -

[2]" The CNAorporation [US]"(2016) *https://www.cna.org/cna-Files/pdf/dop-2016-4-014231-1rev,pdf.*

[3]*- Ibid*

مهارات القراصنة الروس معروفة في جميع أنحاء العالم، إذ " يخطىء من يعتبر روسيا خصما محتملا ضعيفا بعد أن جعل الرجال الحكيمون مجد روسيا مرتبطا بتقنيات الحاسوب "[1].

تقوم الإستراتيجية الروسية على أساس إستراتيجيات الردع بالهجوم، فطالب السنة الأولى قسم علاقات دولية يتعلم معنى الردع منذ أول حصة.

كما تركز روسيا بالأخص على نجاح العمليات الإعلامية التي تقودها على شبكات التواصل الإجتماعي، ورغم الإتهامات المتوالية لها من أطراف دولية عدة إلا أنها مستمرة في هذا النمط الناجح من النشاط الهجومي بالنظر إلى أنها إستطاعت النجاة من أي تبعيات فعلية لعملياتها السيبرانية حتى الضخمة منها بسبب صعوبة تعقب الجناة .

و تسعى روسيا لزيادة القدرة الدفاعية السيبرانية بتطوير طرق ووسائل التحايل على نظم مكافحة الفيروسات و دفاعات الشبكات و أنظمة التشغيل من خلال تشجيع القطاع الخاص و الأفراد على المساهمة في حل المشاكل التقنية و التكنولوجية و تعد هذه الإستراتيجية المحكمة إمتدادا لإستراتيجية الحرب الإيديولوجية في وقت إتحاد الجمهوريات الإشتراكية السوفياتية[2] أين إستخدمت الهجمات النفسية كسلاح فعال لاحباط الأعداء و ثني عزائمهم ، و هو الأمر الذي أوضحته الشراكة الروسية مع ويكيليكس و التي تسببت في تسريب هائل عدد من الوثائق السرية التي لم تضر بالولايات المتحدة الأمريكية فحسب بل بالدول الغربية و دول العالم عموما.

للإستراتيجية الروسية إمتدادات تاريخية في الحقبة السوفياتية عبر عنها رئيس هيئة الأركان العامة الروسية فاليري جيراسيموف ب " الطرق غير المباشرة و غير المتماثلة و قد صدرت وثيقة وزارة الدفاع الروسية المعنونة ب: "مفهوم الأنشطة الفضائية للمعلومات للقوات المسلحة بالإتحاد الروسي سنة 2012" أو مايعرف عند الغرب بعقيدة جيراسيموف The gerasiomove doctrine[3]،و التي تتلخص في إستهداف نقاط الضعف لدى الخصوم و تجنب المواجهة حتى المراحل النهائية من الصراع ، و هو ما يبرز سعي موسكو الحثيث من أجل استعادة إرثها التقليدي من النظام الدولي حيث أكدت الوثيقة المعلومات كأساس لأمن الدولة و كانت هذهالأطروحات شرعنت الاستخدامالعسكري لمجموعة واسعةمن الأنشطة و العملياتو الأدوات غير المتناظرة للحد من القدرات الغربية العسكريةو استغلال الثغرات الموجودة في المجتمعات الغربية **وقد أثبتت روسيا براعة في استخدام التضليل المعلوماتي.**

المطلب الثاني : تهديدات الأمن القومي الروسي

يعد نشاط القراصنة الروسي لكسب المال غير القانوني من أهم تحديات الأمن الرقمي الروسي حتى أن شركات أمن الكمبيوتر و بهدف اختبار أمنها تعين كثيرا من " مخترقي شركات

[1]-" L'otan se prépare à une guerre cybernétique contre la russie, (2012) , octobre 20 2012 https://www.alterinfo.net/L-OTAN-prepare-une-guerre-cybernetique-contre-la-Russie_a82691.html

[2]- محمد بسيوني،" عقيدة جيراسيموف : دوافع الإستراتيجية الروسية لحرب لمعلومات ضد الدول الغربية"، الصباح الجديد، مركز المستقبل(2017)،آخر تحديث 23 أكتوبر 2017 https://futureuae.com/ar/Mainpage/Item/3371/

- محمد بسيوني،" عقيدة جيراسيموف "،مرجع سابق

أمن الكمبيوتر"، و يتركز معظم نشاطها مع وكالة المخابرات الروسية FCB إظافة لتطور نشاط التجسس الرقمي و نمو التهديدات الرقمية التي تشكلها المنظمات الإرهابية و هو الخوف الذي أكدته مصادر في أمن البنية التحتية الروسية و التي تشير إلى " الخوف من الفيروسات التي يمكن أن يتم تصميمها ليس فقط لسرقة بعض المال، بل في الواقع يتم " استخدام الأسلحة السيبرانية بانتظام ضد روسيا"، و رغم أن مجتمع الأمن السيبراني يحاول إبقاء هذا النوع من الهجمات خارج المعرفة العامة إلا أن شركات إنفاذ القانون و الأمن قامت بالتبليغ عن هجمات ضد الحكومة الروسية سنة 2013 عندما هوجمت روسيا بسلاح " سبوتنيك"[1] الذي صمم لتنفيذ التجسس السيبراني من خلال حجب المعلومات عن أنظمة الوكالات العسكرية و المعاهد و المنظمات الدبلوماسية و ذلك عبر استغلال الضعف في برامج مايكروسفت أوفيس ويندوز و رد أكسل و أوتلوك.

و رغم إستحالة تتبع أين تم إرسال المعلومات المسروقة لأن الوجهة كانت مخفية وراء سلسلة من خوادم "البروكسي" إلا أن البحث قاد إلى أن البيانات المسروقة تهم أعداء روسيا الجيوسياسية. مما يعني أن دخول " الحرب الرقمية كشكل من أشكال المواجهة بين الدول بلغ مرحلة نشطة"[2].

ففي جويلة 2016 أعلنت إدارة الأمن الفدرالي الروسي " فسب" FSB أنها اكتشفت اختراق البنية التحتية المعلوماتية ل 42 شركة من مؤسسات تابعة للدولة والعلوم والدفاع و أفادت نفس المصادر أن الهجوم كان مخططا بعناية مما يعني قيام مهنين مؤهلين بالعملية.

وقد تم رصد تصميمات مختلفة للهجمات المنفذة بحيث يتم استهداف كل شركة بشكل منفرد مما يعني أن الضحايا كانوا مصابين بالتصيد الاحتيالي ، و خلصت اللجنة البرلمانية للأمن القومي الى أن هذا التجسس الرقمي " مفيد في المقام الأول للأمريكيين" . كما يخشى رجال السياسة الروس اختراق المراسلات الخاصة بهم بعد أن تم اختراق حساباتهم الخاصة على البريد الإلكتروني حتى ان صناع القرار الروسي و رجال السياسة عامة يستغنون عن حمل هواتفهم النقالة أثناء الاجتماعات الهامة لتجنب التجسس على محادثتهم .

و هو الأمر الذي دفع الحكومة الروسية للتفكير بجدية في حماية المحادثات الهاتفية عام 2017 ، حيث صممت نظام gyptophone الذي يتيح للمستخدمين إجراء مكالمات هاتفية آمنة كرد فعل لإصدار الرئيس الأمريكي السابق أوباما لأوامر بتطوير أسلحة سيبرانية ضد روسيا و هي العملية التي انطوت على عمليات . "زرع" في البنية التحتية الإلكترونية الروسية و التي يمكن تشغيلها عند اللزوم لتعطيل الأنظمة الروسية و قد كان لذيوع خبر ما يسمى ب " المعادل الرقمي للقنابل" كبير الأثر على سرعة اتخاذ التدابير المتعلقة بالحماية الالكترونية[3].

---

[1]Ibid," L’otan se prépare à une guerre "

[2] - "Federeca Fazio-from cold war to cyberwar :the future of US- Russia relations " ,Aspenia(2016),21 décembre2016
https://www.aspeninstitute.it/aspenia-online/article/cold-war-cyber-war-future-us-russia-relations

[2] -Comment le gouvernement russe se prépare la cyberguerre à veunir ?" ,Mediapart(2017),modifié le 31 juillet2017
https://blogs.mediapart.fr/grandfach-xcom/blog/290717/enquete-comment-le-gouvernement-russe-se-prepare-la-cyberguerre-venir

[3] -Ibid, "Comment le gouvernement russe "

إن الإستخدام العسكري لمجموعة الوسائل و الحقائق من الأنشطة و العمليات و الأدوات غير التناظرية للحد من القدرات الغربية العسكرية و إستغلال الثغرات الموجودة في المجتمعات الغربية هي المعادلة التي تعتمد عليها الحكومة الروسية لضرب أعدائها.

المطلب الثالث: محددات التفوق الرقمي الروسي

أولا:عوامل القوة السيبرانية وقوة الجيش الروسي:

أ- عوامل القوة السيبرانية

لدى موسكو قوة سيبرانية رائدة و ذلك يعود لعدة عوامل اهمها:

1-الإستثمار الكبير في نظم الدفاع المعلوماتية، إذ تتبوأ وكالة زيكوريون الروسية الاستشارية[1] لتحليل المعلومات مرتبة متقدمة من حيث خدمات القرصنة.

2-زيادة تمويل قدرات الانترنت الدفاعية: خاصة بعد الهجمات الإلكترونية الأمريكية الإسرائيلية على المواقع الإيرانية عامي 2010-2011 إذ تحتل المرتبة الخامسة من حيث الإنفاق بعد الولايات المتحدة الأمريكية و الصين و المملكة المتحدة و كوريا و يتم رصد 300 مليون روبل سنويا لتدعيم الأنشطة السيبرانية.

3-كفاءة الجيش السيبراني الروسي: وصلت قوات الأمن الالكتروني الروسي مؤخرا إلى 1000 موظف و قد حدد الجيش أهدافه فيما يلي :

- التجسس:

- الهجمات الإلكترونية التي سببت أضرارا بليغة للبنى التحتية الإقتصادية و الأمنية للبلدان الأجنبية.

- الإضطلاع بحروب المعلومات في وسائل الإعلام و على الشبكات الاجتماعية[2].

- منع الهجمات المعادية: حيث أكد أوليانوف أن العقيدة الأمنية الروسية تركز على "الدفاع و ليس الإساءة" فالجيش السيبراني الروسي يركز في المقام الأول على.صد الهجمات الإلكترونية و على وقف ثورات تويتر. فقد إستطاع أن يحبط هجمات الكترونية استهدفت القطاع المصرفي في روسيا بعد أن إستهدف القراصنة الأجانب نظام الإئتمان المالي بخلق أ...........زمة تجبر الشركات على الإفلاس مما تسبب في فوضى كبيرة لدى البنوك الروسية بعد فقدها لتراخيصها. وقد واجهت الحكومة الروسية الأزمة بشراء آلات كاتبة آمنة في المكتبات الحيوية و السرية حتى لا تتعرض هذه الأخيرة للاختراق بدورها.

- الإستثمار: أطلقت وزارة الدفاع الروسية " دعوة لتقديم عطاءات للدراسات حول أمن الكمبيوتر"[1]ويهتم الجيش الروسي بطرق و وسائل التحايل على نظم مكافحة الفيروسات و دفاعات

---

[1] - "ما هي أفضل خمسة جيوش الكترونية في العالم و ماترتيب الجيش السيبراني الروسي"، KATEHON.(2017)،آخر تحديث13جانفي2017 http://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy

[2] - مرجع سابق.

الشبكات و أنظمة التشغيل، و تهدف هذه الدعوات لتشجيع المواطنين الروس للمساهمة في حل المشاكل العلمية والبحثية و تشجيع القطاع الخاص في إطار إستثمار تكميلي تنظيمي مبدع.

ب- قوة الجيش الرقمي الروسي: http://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy

حسب وصف سيرجي تشويجو فإن الجيش السيبراني الروسي أكثر قوة و فعالية من أجهزة المخابرات في الجيش[2] و هو ما يعبر عن الرؤية الخاصة بالرئيس الروسي الحالي فلادمير بوتين الذي يعتبر هزيمة العدو في المجال الرقمي احدى أولوياته العسكرية و السياسية. ولا يستخدم منظروا الجيش الروسي مصطلحات الانترنت أو السيبرانية أو حتى الحرب الإلكترونية و بدلا من ذلك فإنهم يقومون بتصور العمليات الإلكترونية داخل نطاق أوسع أي في إطار "حرب المعلومات"

كما تتبوأ وكالة زيكوريون الإستشارية و التي مقرها موسكو مرتبة عالية في مجال خدمات القرصنة و يعد الجيش الروسي واحدا من أفضل خمسة جيوش سيبرانية في العالم. و قد زادت روسيا تمويل قدرات الجيش السبرانية خاصة بعد الهجمات الإلكترونية الأمريكية و الإسرائيلية على المواقع النووية الإيرانية عام 2010. وقد صرح أوليانوف أن" لدى روسيا "قوة أنترنت رائدة"، وقال ديميدوف أنه " لا توجد وسيلة فعالة لمواجهة مثل هذه التكنولوجيا اليوم" [3] .

ثانيا:مقاربة حرب المعلومات الروسية:

ترتكز مقاربة حرب المعلومات الروسية على:

- خلق بيئة متسامحة dermessive environnement تهدف لتخفيف حدة المقاومة والتأثير في الرأي العام فسياسة موسكو تتجسد في دعم بزوغ قوى اليمين المتطرف في أكثر من دولة غربية حيث تظهر هذه القوى علاقات تعاون كبيرة مع موسكو[4].
- تعويض القدرة على المواجهة: عبر إضعاف الخصوم بتعطيل إستجابتهم للغزو الروسي.
- تشويه صورة القوى المناهضة و بالمقابل تشييد صورة إيجابية لحلفاءها عبر توظيف الأدوات الدعائية المعلوماتية التي تستعمل لخدمة هذه الأغراض.
- إثارة المشاكل الداخلية بالتكريس لأوضاع داخلية متأزمة في المجتمعات الغربية كالضغط على ألمانيا لفتح ملف اللاجئين و إثارة قضية الفتاة الألمانية[5].
- مواجهة العقوبات الغربية: قامت روسيا بالتدخل في أكرانيا عام 2014 و ضم شبه جزيرة القرم و بعد إستفتاء مارس 2014[6] و تزايدت العزلة الأوربية المفروضة على روسيا مع استمرار

---

[1]Ibid."L'otan se prépare à une guerre cybernétique contre la russie "

[2]- "La russie crée un armé cybernétique",yandex(2017) , 24 fevrier 2017
https://infosdanyfr.wordpress.com/2017/02/24/la-russie-cree-une-armee-cybernetique/

[3] - "ما هي أفضل خمسة جيوش الكترونية في العالم و ماترتيب الجيش السيبراني الروسي"، مرجع سابق

2- مرجع سابق

3-بسيوني، " عقيدة جيراسيموف"، مرجع سابق

[6] - شفيق ، نوران. "أشكال التهديدات الالكترونية و مصادرها ". المركز الأوروبي لدراسة مكافحة الارهاب و الاستخبارات(2017) .آخر تحديث 10 ديسمبر 2017.
https://www.europarabct.com/B1%D9%87

إظهارها لإصرار قوي للحفاظ على نفوذها التقليدي في الدول التي كانت ضمن المجال السوفييتي سابقا.

- و تعد محاولة الغرب لإستقطاب هذه الدول دافعا قويا لروسيا لتكريس مرحلة الحرب الهجينة Hybrid warfare و التي تمتزج فيها الأدوات التقليدية و غير التقليدية في تعاطيها مع الغرب[1].

وتركز روسيا بمساعدة المتعاطفين معها على الخلافات السياسية و الثقافية التي تطبع الولايات المتحدة الأمريكية إذ استغلت البرمجة المتطورة لفيسبوك و جوجل لتغذية التضليل الإعلامي لدى المواطنين الأمريكين مستغلة قابليتهم لتصديق الأكاذيب بنشر إعلانات مغرضة على الأنترنت يراد بها تأجيج الشقاق و الخلاف متخذة أكثر المواضيع إثارة للجدل كالإجهاض و امتلاك المدنين للأسلحة و المساواة بين الجنسين و العنصرية مواد مغذية لنار الخلاف المستعرة.

و لقد كانت الشراكة مع ويكيليكس منبرا بث عبره دعايات مغرضة على حسابات تويتر المؤثرة مثل حساب الرئيس الأمريكي كما قام الروس بإنشاء آلاف الحسابات الزائفة على الانترنت بثت عبرها ملايين التعليقات المحرضة تسببت بحمى سياسية أدت لغليان الوضع السياسي الأمريكي، إن عبقرية هذه الحرب الرقمية هي أن الأمريكيون يقومون بمعظم العمل فيها بل و تجعل من وسائل الإعلام الأمريكية من ضمن وسائلها كالبرامج الحوارية على التلفاز و شبكات الأنباء و في الراديو و كل قنوات الاتصال الرقمي من خلال تداول الإشاعات و الأخبار الملفقة[2].

و تشتد الهجمات في سياق " الحرب الهجينة" بين روسيا و أكرانيا و يصعب تتبع هذه الإعتداءات لمعرفة مصدرها بالضبط لأنها تمر عبر عدة خوادم لعدة أنظمة وفي عدة بلدان و لكن على ضوء تحديد أنواع البرمجيات الخبيثة المستخدمة و المجموعات ذات الصلة بالهجمات فيبدو تورط روسيا أمرا أكيدا.

إن الأحداث في أكرانيا ما هي إلا تنبؤ لصراعات القرن الواحد و العشرين بعد أن صرفت الولايات المتحدة الأمريكية أكثر من 5 ملايين[3] دولار لمساعدة أكرانيا على تطوير دفاعها الإلكتروني وتتخذ الولايات المتحدة من حلف الناتو واجهة لها للتصدي لروسيا إذ يدرك الغرب جيدا أن ما يحدث في أكرانيا ما هو الا مجرد تنبؤ لصراع مستقبلي وشيك لهذا النوع الجديد من الحرب" و يتزايد القلق لدى الولايات المتحدة الأمريكية من أن تحذو دول حذو روسيا.التي يبدو أنها تمتلك الأفضلية في ترتيب هذا التنافس فهي ظل سيطرتها الدائمة على المبادرة بالهجوم .

ثالثا: الخبرة الرقمية العملية الروسية: نماذج

-في الشيشان:

---

[1] - بسيوني،"عقيدة جيراسيموف"، مرجع سابق.

[2] - Ibid" la Russie crée une armée "

[3] - Sébastien Gobert, "Ukraine,veritable laboratoire de la guerre cybernetique", les voix du monde RFI(2017), modifié le 11 octobre 2017
www.rfi.fr/emission/2017-ukraine-veritable-laboratoire-gurre-cybernetique

لقد اكتسب الروس خبرة لا يستهان بها في مجال العسكرة الرقمية إذ كانت حربهم في الشيشان و الدعاية القوية و المؤثرة التي استخدمها الشيشانيون عام 1994 و البروباغندا التي شهدها الانترنت وقام بإدارتها الجهاديون الشيشانيون مثلث الكبوة التي تم التغلب عليها فيما بعد، اذ أنه في حرب الشيشان الثانية سنة 1999 قامت روسيا بتصعيد عملياتها في الفضاء السيبراني ضد الشيشانين بناء على تعليمات بوتين عندما كان نائبا أول لرئيس الوزراء حينها و الذي أمر بتطوير تكتيكات الحروب السيبرانية، ورغم أن هذه العمليات كانت تجري كلها في اطار الحرب النفسية الدعائية الا انه سرعان ما تطور الامر عندما قامت جماعات معادية للناتو والغرب عموما باستهداف البنية التحتية للشبكة العنكبوتية في حرب كوسوفو، فقدت شنت جماعة اليد السوداء (black hand) هجماتها على شبكة الكمبيوتر العسكرية للناتو و الولايات المتحدة الأمريكية و استطاعت اختراق عدد من الأجهزة ومسح البيانات المخزنة عليها[1].

- في استونيا:

لم يهتم القادة الروس بضم الفضاء السيبراني للعقيدة العسكرية للجيوش النظامية شأنهم شأن الدول المعنية بالتهديد الرقمي حتى نهاية 2007 عندما اشتعل الغضب الروسي اثر قيام دولة استونيا بتحويل النصب التذكاري السوفيتي للحرب العالمية الثانية من تالين العاصمة الاستونية ، الامر الذي دفع بروسيا لشن سلسلة من الهجمات الرقمية الواسعة و التي استهدفت البنية التحتية الاساسية لاستونيا و حولت البلاد لمختبر حقيقي للحرب السيبرانية بين الولايات المتحدة و الدول الحليفة لهامن جهة وروسيا من جهة أخرى[2].

-في جورجيا و أكرانيا:

خلال حربها القصيرة الأمد في جورجيا عام 2008 نجحت روسيا في تعطيل حواسيب المؤسسة الحكومية الجورجية اذ نجحت باختراق مواقع اعلامية حكومية في أكرانيا التي تدهور فيها الوضع في فيفري 2014 اثر الثورة التي اسقطت حكومة يانكوفيتش الموالية لروسيا، و قبل 4 أيام من الانتخابات الرئاسية أي تحديدا في ماي 2014، قامت موسكو بسلسلة اعتداءات رقمية طالت حواسيب لجنة الانتخابات المركزية الاكرانية[3] مّما ادى لتوقفها كليا عن الخدمة، و لم ينته الأمر عند هذا الحد بل و في يوم التصويت نفسه تم اختراق موقع اللجنة الانتخابية وقام التلفزيون الروسي ببث نتائج مزيفة قبل إعلان النتائج الرسمية مباشرة.

وقد دفعت هذه الانتهاكات الروسية بالحكومة الأكرانية لاعتماد التصويت الشخصي و الفرز اليدوي مّما أحبط المخطط الروسي القاضي بالتأثير في نتيجة الانتخابات.

---

[1] - Mansur Mirovalev," Chechnya ,Russia and 20 years of conflict" ,Newsgrid(2014)diffusion11décembre2014 https://www.aljazeera.com/indepth/features/2014/12/chechnya-russia-20-years-conflict-2014121161310580523.html

[2]- Damien McGuinness," haw cyber attak transformed Estonia", BBC News(2017), modified April 27, 2017
https://www.bbc.com/news/39655415

[3] -Christopher Miller,"what's Ukraine doing to combat Russian cyber warefare ? Not enough " Radio Liberty(2018), modified march 07,2018
https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html

-في المجر وبولندا[1]:

كانت روسيا أكثر حظا في المجر عندما تمكنت من تسريب تسجيل سري لخطاب رئيس الوزراء المجري امام اعضاء الحزب الاشتراكي عام 2006 بما ساهم في تراجع شعبية الحزب وتحقيق الفوز الكاسح لحزب فيكتور أوربان اليميني المتطرف المقرب من موسكو في انتخابات 2010.

وهي نفس الاستراتيجية التي اتبعتها في بولندا عندما أدى بث المحادثة الخاصة التي جرت بين وزراء في الحكومة البولندية في أحد مطاعم وارسو إلى تراجع كبير في شعبية حزب " القانون الحاكم " حينئذ وتسبب في فوز حزب " القانون و العدالة" اليميني المتطرف المعادي للاتحاد الأوربي و المقرب من موسكو في الانتخابات العامة الأخيرة.

ينبغي الاشارة إلى أن هناك اتفاقا عاما واسعا لدى المسؤولين الحكوميين الغربيين و في وسائل الإعلام الغربية أيضا على " النجاح الاستثنائي" للإستراتيجية السيبرانية الروسية، و التي عبر توظيفها لمجموعة وسائل متنوعة بدأً من التجسس التقليدي مروراً بالهجمات الرقمية وصولا لحملات البروباغندا الإعلامية الممنهجة في وسائل التواصل الاجتماعي التي تهدف للتأثير في الرأي العام للدول الغربية وجيرانها بغرض زعزعة الثقة في حكوماتها وبتدعيم الحركات السياسية الموالية لها وبث الاخبار الكاذبة و التسريبات الهامة ، أكدت أن نجاح الاستراتيجية الروسية لا يتعلق بالتفوق الروسي التقني و المخابراتي المعروف فحسب، بل يعود في شق كبير منه للإدراك العميق و الفهم الشامل لخصائص البنية التحتية الرقمية المتسمة بالتمدد الكثيف عالميا و الاعتماد عليها من طرف المؤسسات الحكومية و الحزبية خاصة في تنفيذ عملياتها الديمقراطية ،و هو ما عبر عنه القادة الأمريكيون عندما صرحوا بأن "روسيا متقدمة على هذا الصعيد لأنها عرفت كيف تستخدم حرياتنا ضدنا و لا يمكننا فعل الكثير بهذا الشأن".[2]

وتجدر الإشارة إلى أن ما يسمى بالاستفزازات الروسية لم تقتصر على الولايات المتحدة الأمريكية فحسب بل امتدت لتطال حلفاءها الغربيين كالمملكة المتحدة و فرنسا وكذلك المانيا حتى أن الولايات المتحدة الأمريكية تدرس الردود الملائمة و المناسبة لمواجهة الأنشطة العدائية الروسية ضد الاتحاد الاووربي و منظمة شمالي حلف الأطلسي أو ما يسمى "بالتطاول الروسي" كدعوة رئيسة الوزراء البريطانية تيريزا ماي لتشكيل حكومة حرب.

المبحث الثاني: العسكرة الرقمية الأمريكية

المطلب الأول: السياسة الرقمية الأمريكية

أولا: التحول في العقيدة العسكرية الأمريكية

إن الفشل العسكري في تحقيق الأهداف الإستراتيجية للحروب التي تديرها الولايات المتحدة الأمريكية واكب التغيرات التي طبعت الساحة الدولية بسبب الإنتشار الرقمي.

---

[1] - "الحرب الباردة مستعرة في الفضاء الالكتروني "، صحيفة العرب (2017)، آخر تحديث 13أكتوبر2017.
الحرب- الباردة- مستعرة- في- الفضاء- الالكتروني/ https://alarab.co.uk

[2] - مروة الأسدي ، " "،مرجع سابق

فعدم قدرة الجيش الأمريكي على حسم أو ربح الحرب الإقليمية[1] غير التقليدية التي تخوضها جماعات مسلحة صغيرة عزز من إدراك الولايات المتحدة بأن فلسفة الحرب القادمة تعتمد على العدو المركب بمزدوجي الدول المعادية و الفاعلين غير الحكوميين، و مع دخول أمن الانترنت على الخط العام للإستراتيجية العسكرية و توسيع دائرة التضييق على الحريات العامة، تأثر شكل العمليات العسكرية المحتدمة و التي تحولت من عمليات حروب نظامية إلى " عمليات شبحية مفتوحة و مهام عسكرية محدودة" [2]بل ان القتال أضحى يتم عن بعد بالطائرات المسيرة القليلة الكلفة و التكلفة، أن هذا التحول النوعي في القدرة العسكرية حول من الإستراتيجية العسكرية الأمريكية إلى استخدام المرتزقة البديلة و القدرة المكتسبة و التي تعد تكاليفها المادية و البشرية أقل بكثير من تكلفة الجيوش النظامية.

إن الإتجاه نحو استخدام القوة الافتراضية لم يكن وليد اللحظة بل جاء نتيجة الفشل العسكري الذي منيت به الولايات المتحدة الأمريكية في العراق[3]، كما أن الطفرة التكنولوجية التي حدثت في مجال الاتصالات مكنت من اختصار الجهد و الزمن من أجل إيصال المعلومة و الفكرة بمتغير الانترنت الذي جعل من شبكات التواصل الإجتماعي أداه فعالة أحسنت الولايات المتحدة إستخدامها في أسلوبها المعتمد لاحداث التغيير في البلدان العربية إبان الانتفاضات الأخيرة.

لقد برز مصطلح القوة الذكية كمنهج جديد في الساحة الخارجية الأمريكية خلال الفترة الرئاسية لباراك أوباما أين سجل سعي العديد من المفكرين منذ بداية رئاسته للترويج له، نذكر من بينهم: جوزيف ناي، زبيغو بريجنسكي، ريتشارد أرميتاج، والذين حاولوا تطوير نظام الأمن القومي بشكل جذري وهو السعي الذي ترجم من قبل وزيرة الخارجية السابقة هيلاري كلينتون في ترسيخها لمفهوم القوة الذكية كمنهج جديد يصلح اعتماده لحل المشاكل العالمية و الذي smart power لا يتحقق دون تعزيز دور القوة الأمريكية المدنية وتوسيعها إلى أبعد حد ،و هو ما يحول الرؤيا السياسية من تكديس للترسانة العسكرية و استعراضها نحو حشد للقدرات و المهارات الثقافية و المعلوماتية،الى الإتجاه نحو إستخدام القوة الإفتراضية بعد أن " إكتسب الرأي العام في عصر المعلومات أهمية إضافية حتى في الدول الشمولية" [4]و ظهر جليا تأثير الجهات غير الحكومية على الأحداث الجارية مما إستلزم بلورة للعلاقات لا مع الحكومات فقط بل مع الشعوب أيضا.

و رغم أن نهج القوة الذكية في السياسة الخارجية الأمريكية لم يأت أكله بعد الا أن عسكرة الفضاء الرقمي سمحت باظهار مميزات هذا النهج[5].

ثانيا: الإستراتيجية الدفاعية الرقمية الأمريكية الجديدة:

---

[1] ـمهند العزاوي ،"الاستراتيجية الأمريكية بين مزدوجي المهارشة و القدرة المكتسبة"، العرب نيوز (2010)آخر تحديث 0420 أفريل 2010.
www.alarabnews.com/show2.asp?NewId=24995&PageId=12xPartId=1

2-سيف الهرمزي، "مقتربات القوة الذكية الأمريكية كآلية من آليات التغيير الدولي: الولات المتحدة نموذجا" المركز العربيللأبحاث و دراسة السياسات ، الطبعة الأولى(2016)أطلع عليه بتاريخ 20 أفريل 2018

3- مرجع سابق

[4] - سيف الهرمزي،"مقتربات القوة الذكية " مرجع سابق

[5]- "مصطلح القوة الذكية نهج جديد في السياة الخارجية الأمريكية خلال فترة أوباما " ،مركز الروابط(2014)،آخر تحديث 03 نوفمبر 2014
http://rawabetcenter.com/archives/977

أعلنت وزارة الدفاع الأمريكية في جوان 2011 عن إستحداث قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية و تنفيذ هجمات في الفضاء الرقمي و التي دخلت العمل في شهر أكتوبر من العام نفسه[1].

و تنظر ذات الوزارة للحرب المعلوماتية على أنها " تلك الأعمال التي تتخذ لإحراز التفوق المعلوماتي بمساعدة الإستراتيجية القومية الأمريكية للتأثير سلبا على معلومات العدو و نظم معلوماته و حماية ما لديها من معلومات و نظم"[2]

و ما تفتأ الوزارة تحذر من الهجمات الإلكترونية التي تتربص بالبلاد فحسب ليون بانيتا وزير الدفاع الأمريكي فإن روسيا تمثل الجهة الأجنبية التي تحاول دوما إيجاد ثغرة في الشبكات الإلكترونية الأمريكية شديدة الحيوية والتأثير.

وتقدر الجهات الأمنية الأمريكية أن تأثير الهجوم االرقمي الروسي المرتقب يوازي في حال نجاحه هجوم قاعدة "بيرل هاربر" الذي حدث سنة 1941.

و هو التعبير الذي يدل على الذعر الأمريكي الذي سيطر بعد إختراق جماعات متشددة لمواقع مهمة، حيث تم استبدال أكثر من 30 ألف جهاز أصيب بالفيروس في آرامكو[3] بعد أن أصبحت عديمة الفائدة.

وقد وضع الجيش الأمريكي مواجهة المعسكر الشيوعي القديم (الصين و روسيا) في محور إستراتيجية الدفاع الجديدة في إشارة إلى تحول الأولويات الأمريكية من التركيز على قتال " الجماعات الإسلامية" بعد أكثر من عقد و نصف.

و تمثل هذه الإستراتيجية إصرار الرئيس ترامب المتزايد على مواجهة التحديات التي تطرحها روسيا و الصين رغم دعواته المتكررة لتحسين العلاقات مع موسكو و بكين[4] فالرغبة الأكيدة لروسيا لتشكيل عالم يتسق مع نموذجها السلطوي و اكتساب سلطات تتيح لها نقض قرارات الدول الأمنية و الاقتصادية، مثلث حافزا للولايات المتحدة لمجابهة الخطر المحدق خاصة وأن " روسيا أكثر جرأة من الصين في استخدام القوة العسكرية" على حد قول البريدج كولبي نائب مساعد وزير الدفاع للشؤون الإستراتيجية و تطوير القوات الأمريكية[5].

و هو ما يستدعي العودة إلى أساسيات إحتمال نشوب حرب و هي الإستراتيجية التي ترى بأن التركيز يكون لاعطاء الأولوية " للاستعداد لخوض حرب خاصة مع قوة كبرى"[6] و قد تجسد هذا الأمر في فيفري 2015 عندما أنشأت الإدارة الأمريكية " مركز الاستخبارات المتكامل

---

[1] - عادل عبد الصادق ،"أمريكا و تشكيل قيادة عسكرية في الفضاء الإلكتروني: هل بدأ الإستعداد لحروب المستقبل ؟"،مركز الأهرامات للدراسات ،السكينة ، آخر تحديث 31 أوت 2011 . https://www.assakina.com/news1/9379,html

[2] - "وزير الدفاع الأمريكي ليون بانيتا يحذر من هجمات الكترونية شديدة الخطورة قد تتعرض لها بلاده"،الجزيرة (2012)،آخر تحديث15.10.2012

[3] - مرجع سابق

[4] - سارة عبد العزيز، الحرب السيبرانية "،مرجع سابق.

[5] -" مواجهة روسيا والصين في صلب استراتيجية البنتاغون الجديدة "، RT(2018) ، آخر تحديث 19 جانفي2018 https://arabic.rt.com/world/922151-مواجهة-روسيا-والصين-في-صلب-استراتيجية-البنتاغون

[6] - إسماعيل قادير، مرجع سابق ص13.

للتهديدات السيبيرانية". The cyber threat intelligence intergration (center CTIIC) تحت إشراف مدير الإستخبارات الوطنية (PNI) و يختص بتقدير التحليلات المتعلقة بتهديدات الأمن السيراني و مختلف الحوادث التي تمس بالمصالح الوطنية. كما يعمل على دعم الجهات الحكومية ذات الصلة و منها وزارتا الدفاع و العمل.[1]

و قد أدى إكتشاف فيروس "FLAME" فلايم إلى الوعي بأن الخطر الذي كان في الماضي يمكن درئه بوضع "جدران حماية" حول بنية حاسوبية حاسمة لابعاد الاعداء، لا يكون دون القدرة

على حماية الأنظمة الحيوية الأمريكية من الداخل لذا قامت وزارة الدفاع الأمريكية بإصدار " الإستراتيجية السيبيرانية المحدثة" و التي إحتوت على بيانات أكثر تفصيلا عن القدرات الهجومية الهادفة لتعزيز الأمن السيبيراني هو ما يعني احداث نقلة نوعية لحماية الأصول الداخلية من أجل تعزيز الردع ضد الإعتداءات الرقمية المتكررة.

ثالثا:الإستراتيجية السيبرانية للولايات المتحدة الأمريكية :

تطمح الولايات المتحدة الأمريكية لتحديث إستراتيجيتها السيبيرانية بانتهاج أساليب محددة:

أولها: إعلان الفضاء السيبيراني مجالا تشغيليا للجيش الأمريكي و بناء عليه تم تدشين أكبر قيادة دفاعية سيبرانية في العالم و هي القيادة السيبرانية الأمريكية (USCYBERCOM) و التي ضمت الوحدات السيبيرانية في القطاعات الدفاعية الأخرى.

ثانيا: إصدار استراتيجية العمل في الفضاء السيبراني" من طرف وزارة الدفاع: و قد تضمنت محاور أساسية هي:

- إعتبار الفضاء السيبراني كغيره من مجالات الحرب التقليدية.
- إعتماد الوزارة على أحدث الطرق الدفاعية الجديدة للتعامل مع التهديدات السيبرانية.
- تشجيع التعاون الوطني و الدولي.
- التركيز بشكل كبير على الدفاع كاستراتيجية الكترونية أولية[2]

و قد رسمت الوزارة خطة التحديث معتمدة على :

1- تقاسم مبدأ الحفاظ على الأمن في العالم مع الدول الحليفة لمواجهة تراجع نفوذها العسكري أمام روسيا.

---

[1] -سارة عبد العزيز ،"الحرب السيبرانية"،مرجع سابق

[2] -Ellen Nakashima," List of cyber- weapons developed by the Pentagon to streamline computer warfare ",Wachington Post(2011),modified may 31 , 2011 https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html?noredirect=on&ut

2- إقرار التغيرات العاجلة على نطاق واسع و الذي قام به وزير الدفاع الأمريكي جيم ماتيس والذي مثل السعي الحثيث لتدارك التراجع خاصة و أن الرئيس ترامب أعلن عن إهتمامه بتطوير التكنولوجيا و وجوب الإستثمار فيها كمحور أساسي من محاور إستراتيجيته الجديدة.

3- التكنولوجيا التنافسية : و بغية درء العجز الذي تعترف به الولايات المتحدة الأمريكية للحاق بركب التطور المعلوماتي بعد أن أقرت الأوساط العلمية حاجتها لخمس سنوات على الأقل [1] كي تصبح قادرة على حماية بنيتها التحتية المعلوماتية بشكل يؤمن أمنها السيبراني.

المطلب الثاني: تحديات الإستراتيجية الأمريكية:

هناك توجه يعزز قصور المنظور التكتيكي الدفاعي الأمريكي في مواجهة الأخطار السيبرانية إلى الفهم الخاطئ للقيادة السياسية و العسكرية الأمريكية للخصم المراد مواجهته: و هنا يجب الإعتراف أن الفهم الواضح لسلوك الخصوم في المجال الرقمي يعد في كثير من الأحيان تحديا للطبيعة التقنية للحرب السيبيرانية، فالتطور السريع لأدواتها و الآثار المؤقتة التي تحدثها و الطرق السرية التي تستخدم فيها كثيرا ما تؤدي الى حجب دوافع واستراتيجيات الجهات الفاعلة مما يعني أن الجهات المتضررة تضطر للاعتماد على التقارير الإعلامية خاصة و أن التقريرات الجنائية تركز على أصول و نواقل الهجمات الإلكترونية.

إدراك الخصم للخطر الذي يمثله و للتصعيد في الفضاء السيبراني يشوبه نقص كبير في التحليل و هو الأمر الذي يطبع السياسة الامريكية التي تميل إلى إختلاق إفتراضات غير معلومة عن دوافع الآخرين و إحتياجاتهم، إذ يمكن لحساب المخاطرة للولايات المتحدة أن يكون مضللا و في بعض الأحيان خطيرا سواء كان الخصم الفاعل بلدا أم جماعة.

كيف ينظر الخصوم إلى بعضهم البعض و كيف يستوعبون البعد الرقمي في صراعهم، كيفية حساب المخاطر، التصعيد، كل هذا يحدد طريقة وضع الإستراتجيات الفعالة التي يتوجب استخدامها لتحقيق الأهداف المتوخاة. و لذا يسهل استهداف الولايات المتحدة بسبب نقص التحليل في هذا المجال.

و هو النقص الذي حذر منه وزير الدفاع الأمريكي ليون بانيتا الذي تحدث عن "مرفأ بيرل هاربر الكتروني"[2] تضاهي آثاره التدميرية أحداث الحادي عشر من سبتمبر 2001.

> هذه التحذيرات التي أعقبتها هجمات رقمية واسعة النطاق على عدد من المؤسسات المالية الأمريكية في العالم حيث يتم إختراق البنية التحتية الحيوية في أمريكا يوميا سواء كانت أنظمة كهربائية ، أم محطات مائية و القلق يتزايد من إمكانية إستهداف شبكة النقل و التي تهدد بكوارث حقيقة كاستهداف القطارات و تحويل وجهتها نحو وجهات قاتلة و قد كان

---

[1]- ربيع محمد يحي، مرجع سابق ، ص73، 74

[2] -" مخاوف امريكية من هجمات الإكترونية" ،الجزيرة(2012)،آخر تحديث 10 اكتوبر 2012

www.Aljazeera.net/programs /bihind-thenews/2012/10/15/

الهجوم الإلكتروني الضخم على google كبير الأثر في اثارة الفزع من النجاح في استهداف مواقع نووية .

1-استراتيجية الشراكة التكنولوجية : فيروس ستوكسنت نموذجا

-الشراكة الأمريكية الإسرائيلية:

أسفر التعاون الأمريكي– الإسرائيلي في مجال الإلكترونيات عن تطوير سلاح فعال سمي بفيروس ستوكسنت STUXNT الذي يعتبر أحد أعتى الأسلحة الرقمية المطلقة لحد الآن.

و قد غيرت العملية الإستخباراتية المسماة بإسمه ستوكنت " عملية الألعاب الأولمبية"[1] OPERATION OLYMPIC GAMES[2] من ملامح الفضاء الرقمي إذ أصبح أكثر خطورة و قوة من ذي قبل بفعل أن ستوكسنت يعد أول سلاح سسيبراني فائق القوة Cyber super weapon حتى وصف بأنه صاروخ رقمي موجه Digital guided missil لمهاجمة المفاعلات النووية الإيرانية و قد حذر الخبير الألماني رالف لانغنز و هو خبير في نظم التحكم الصناعية من إمكانية حصول جهات و كيانات غير مسؤولة أو إرهابية على هذا السلاح.

و تقوم آلية عمل هذه البرمجية الخبيثة على توظيف فيروسات تصيب نظام الويندوز و تقوم بمهاجمة أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا حيث أنه لا يعمل عشوائيا بل بشكل محدد جدا، إذ بعد إختراقه للأجهزة و الحواسيب يقوم الفيروس بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة سيمنز الألمانية و في حالة وجودها يقوم بتفعيل نفسه و يبدأ بالعمل على تخريب و تدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم و تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط الى محطات توليد الكهرباء و حتى المفاعلات النووية و غيرها من المنشآت النووية الحساسة.

و قد تم اكتشافه في 2010 من قبل " فيروس بلوك آدا" "Virus block ada" وهي شركة أمن مقرها روسيا البيضاء،و رغم أن ستوكسنت صمم خصيصا للهجوم على برنامج " سيمانتيك وين سي سي " أو مايعرف بنظام سكادا (SCADA) أو" التحكم الإشرافي و جمع المعطيات " المصمم من طرف شركة سيمنز الألمانية و المتعلق بتنظيم حركة المرور و خطوط الأنابيب و إدارة المفاعلات النووية و غيرها من المهام التي يتم القيام بها آليا.

إلا أن الخبراء يتفقون على أن هذا الفيروس الخطير أعد خصيصا لضرب هدف صناعي محدد و هو " المنشآت الإيرانية النووية"[3] إذ تتوفر لديه القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة (PLC) كما أنه يقوم بإخفاء التغيرات التي تم تنفيذها.

---

[1] - سيف الهرمزي، "مقتربات القوة الذكية الأمريكية"،مرجع سابق

[2] - "La cyberguerre " ,wikipédia(2018),modifié le 02 juin 2018 https://fr.wikipedia.org/wiki/Cyberguerre

[3] - "البنتاغون يرفع مستوى ادارة الحرب الرقمية من سلاح معاون الى قيادة قتالية مشتركة "، اليوم السابع(2018)،آخر تحديث 21 أفريل 2018 https://www.youm7.com/story/2018/4/21/

فبعد أن كان الهدف الرئيسي هو التجسس على مفاعل "بوشهر" النووي و نقل المعلومات لحاسوب مركزي في ماليزيا، قام بتخريب مفاعل نطنز جنوب طهران وإستطاع إلحاق الضرر بأجهزة الطرد المركزي لتخصيب اليورانيوم في المنشآت النووية الايرانية.

كما امتد أثره ليصيب 45 ألف حاسب آلي في جميع أنحاء العالم ، 60% منها في إيران لوحدها[1] و قد طالت هجماته اندونيسيا و حتى الولايات المتحدة .

و قد سمح فيروس ستوكنت بإعادة المشروع النووي الإيراني سنتين على الأقل للوراء، بعد أن أثر على النظام الصناعي لآلات كبيرة تشبه الغسالات و التي كانت تقوم بتخصيب اليورانيوم بجعلها تدور خارجة عن السيطرة حتى تدمر نفسها آليا.

و قد كانت الخطوة الأمريكية- الإسرائيلية غاية في الجرأة ،إذ يعد ستوكنت أول فيروس يسبب أضرارا في العالم الواقعي بدل الافتراضي.

و بسبب نجاح المشروع المشترك قامت الولايات المتحدة سنة 2012 بتطوير فيروس آخر "Flame" ، و تسبب هو الآخر بالكثير من الخسائر حيث عطل عددا من المنظومات و قد خصصت له الولايات المتحدة أكثر من مليار دولار[2].

2- الخصخصة التكنولوجية :

-تفعيل دور القطاع الخاص:

تنبغي الاشارة الى أن عمليات مكافحة القرصنة الإلكترونية تقتضي السماح بتبادل المعلومات الأمنية الرقمية بين القطاع العام والخاص و هو الأمر الذي يحتاج لتعريف حدود الدفاع عن النفس لكل مؤسسات القطاع الخاص و التي ترغب في المشاركة في عملية محاربة التهديد الإلكتروني بغية الوصول لتطبيق إجراءات أكثر ردعا، بعد إن طالت الاختراقات المتوالية شبكات كبرى حيوية مثل أمازون و فيتفليكس و باي بال، و تمكن المتسللون من إحداث إصابات كبيرة في أنظمة الشبكات المخترقةمما عزز الحاجة الملحة لمواجهة التهديد الرقمي المشترك الذي يفرضه ضعف القدرة الإلكترونية على الاستجابة لمشكلة سرعة الجهات الفاعلة ، و هي إستراتيجية الرئيس ترامب الذي يسعى للحصول على ميزة تنافسية في القطاع الخاص.

و بالنظر للضعف النسبي الذي تشهده النظم المعلوماتية الأمريكية فإن عام 2017 لم يشهد هجمات على الوكالات الحكومية بقدر ما شهدت الشركات الخاصة تكالب القراصنة عليها خاصة أولئك المدعومين من قبل الدول[3]، وهو ما جعل من حتمية تعزيز التعاون و التآزر بين قطاع الأعمال و الحكومة لمواجهة التهديدات السيبرانية المشتركة أمرا لابد منه خاصة و أن ادارة ترامب تبحث عن

---

[1] - ستوكنت، مرجع سابق.

[2] - "Flame :le virus informatif le plus puissant au monde" ,le temps (2012),diffusion 29 mai 2012 https://www.letemps.ch/no-section/flame-virus-informatique-plus-puissant-monde

[3] - عمر نجيب، "الحرب الباردة المتجددة بين روسيا و الولايات المتحدة: معالم ميزان قوى عالمي في طريق التشكل"،رأي اليوم (2018)،آخر تحديث 18 سبتمبر 2017
https://www.raialyoum.com/index.php/- الباردة –المتجددة –بين – روسيا – والولايات- المتحدة -الأمريكياالحرب

"جعل أمريكا قوية من جديد" [1]عن طريق الاستثمار في التكنولوجيا المعلوماتية بعد ما أصبح الاستثمار في صناعات التقنية الحديثة المبنية على المعرفة يشكل جزءا رئيسا من الاقتصاد العالمي[2] .

- **تجارة الأمن الإلكتروني:**

يوما بعد يوم تغدو العسكرة الرقمية عائدا ضخما للإستثمار بعد أن باتت صناعة الامن الالكتروني من واحدة من أسرع الصناعات نموا حول العالم[3]. فزيادة المخاوف و هاجس الأمن الرقمي أدى إلى خلق العديد من الإدارات و المكاسب الحكومية حيث تضاعف وزارات الأمن القومي حجمها عدة مرات كل سنة بغرض تجهيز وحدات مهمتها الوحيدة هي خوض الحروب و النصر في الفضاء الإلكتروني.

و مع بدء المستخدمين فقدان الثقة في أمن و سلامة الانترنت مع عدم إمكانية الإستغناء عنه، برز مصطلح "تجارة الأمن الإلكتروني" بقوة كمصطلح جديد ظهر في عالم الإقتصاد مع توسع شبكة الانترنت في بداية التسعينات من القرن العشرين.

و الذي يعد الإستثمار الأمثل للفرص الإقتصادية التي يتيحها قطاع الطاقة الذكية[4]، فقد أكدت المواقع الإلكترونية قدرتها على صياغة نوع جديد لمفهوم التجارة و الربح المادي حيث بات الإستثمار فيها خليط يدمج بين إدارة و تنظيم هذه التقنيات و تحويلها لتجارة مربحة. إذ برزت عدة شركات سخرت أموالها لخدمة الأمن الإلكتروني

من الاستثمار الالكتروني الى تجارة الامن الالكتروني:

في ظل إتساع نطاق مظاهر الأنشطة العدائية التي يمارسها الفاعلون الدوليون على الساحة الرقمية تصاعد دور الشركات العاملة في مجال الأمن الإلكتروني بنمو صناعة الأمن السيبراني التي تعد من أسرع القطاعات نموا في صناعة التكنولوجيا العالمية و ذلك بحوالي 1.9 مليار دولار اذ بلغت قيمة رأس المال الإستثماري في هذا القطاع خلال عام 2013 مستويات غير مسبوقة فضلا عن مئات الشركات الجديدة المتخصصة فيه[5].

و تمتلك الولايات المتحدة من المؤهلات ما يخولها الهيمنة على القطاع خاصة بعد الإستثمار الكبير في مجال الإتصالات لأغراض إقتصادية بالنظر لمحتويات صناعة الأجهزة اليابانية والكورية و الصينية و الأوربية. كما تظهر الأرقام نشاطا أمريكيا كبيرا فشركة IBM و أبل ومايكروسوفت و فيسبوك تتعامل مع 1.15 مليار مستخدم حول العالم 50 % من مستخدمي الأنترنت.وجوجل

---

[1] - محمد أبو النور ،"استراتيجية المحاور الأربعة :الرئيس الأمريكي يعلن خطة جديدة للأمن القومي..ترامب :الصين وروسيا تعملان ضد مصالح الولايات المتحدة الأمريكية ..و الرؤساء السابقون سبب ضعف واشنطن وتمدد ايران "، اليوم السابع (2017)،آخر تحديث 19 ديسمبر 2017 https://www.youm7.com/story/2017/12/19/

[2] - عادل عبد الصادق، "عسكرة الفضاء الإلكتروني" ،مرجع سابق

[3] - بيتر وارن سيتغر و ألن أ فريدمان، "الأمن الإلكتروني و الحرب الإلكترونية" ،مرجع سابق،04

[4] - عمرو الخالد،"الأمن الالكتروني من أهم مرتكزات اقتصادات الطاقة الذكية "، البوابة العربية(2018) ،آخر تحديث 08 مارس 2018 / الأمن الالكتروني – أهم-مرتكزات-اقتصا/_2018/03/08 /com.aitnews//https

[5] - عزة هاشم، "عسكرة الفضاء، الحروب السيبرانية، أمن الطاقة"، مركز الدراسات الإستراتيجية و الدولية المتحدة (2016) ،آخر تحديث }جانفي 2016 .https://futureae.com/ar/mariage/ttem/659/

لوحدها لوحدها تتعامل مع 26% من مستخدمي الانترنت و تبث 4 مليارات شريط فيديو في اليوم الواحد. و أخيرا تويتر التي تتعامل مع 22 % من مستخدمي الانترنت حوالي 546 مليون تويتري[1].

ومع تحول الصحف كلها لإتخاذ المصادر الأمريكية كمراجع اخبارية ، واستمرار ترحيل الإعلانات ببطىء من التلفزيون إلى الانترنت و الشبكات الاجتماعية ، يتم إستغلال هذه المؤهلات لعسكرة الفضاء الاتصالي بغرض التجسس بدعاوي أمنية، و قد ساعد هذا توفر 70% من أكثر أقوى أجهزة الكمبيوتر و الحواسب الفائقة في العالم. كل هذه المعطيات أهلت الولايات المتحدة الأمريكية لغزو الساحة الرقمية العالمية خاصة بعد ثبوت ضلوع شركات الأمن الإلكتروني في عمليات التجسس وتجنيدها من طرف الدول لخدمة أغراض إقتصادية.

المبحث الثالث: التنافس الروسي -الأمريكي أو الحرب الباردة الجديدة

المطلب الاول: التصعيد الروسي -الامريكي: ردود الفعل الامريكية في ظل الاختراقات الروسية

تعتقد الولايات المتحدة بما لاشك فيه أن التسريبات التي حدثت خلال الحملة الرئاسية لمترشحة الحزب الديمقراطي "هيلاري كلينتون" و التي سيطرت على العراك السياسي آنذاك يقف وراءها شخصيا الرئيس الروسي بوتين كما أن العديد من مسيري و موجهي المعلومات الأمريكية يؤمنون بتورطه في عمليات القرصنة التي طالت الحزب الجمهوري[2].

و بعد توصل الاختراقات الروسية لاستهداف نظام معلوماتي مستخدم من طرف قيادة أركان الجيش الأمريكي تحول الأمر لأزمة دبلوماسية حقيقية، خاصة مع توجه الرئيس السابق باراك أوباما بخطاب شديد اللهجة للرئيس بوتين سنة 2016 ملوحا بعواقب و خيمة يمكن أن تنتج ان لم يتم إيقاف الهجمات الروسية المتكررة وتتهم الولايات المتحدة روسيا بقرصنة قاعدة بيانات لجنة الحزب الديمقراطي بشكل أضر بسمعة المرشحة الديمقراطية "هيلاري كلنتون" و ساعد " بطريقة ما" المترشح الرئاسي آنذاك "دونالد ترامب" للحصول على ميزة أدت لفوزه بمنصبه الرئاسة.

و رغم نفي الحكومة الروسية الاتهامات الأمريكية إلا ان الرئيس بارك أوباما هدد بشن حرب رقمية واسعة النطاق على روسيا بعد أن بات لزاما على الحكومة الأمريكية ردع الاعتداءات الروسية ،بهدف ارسال رسالة واضحة لكافة الدول الأخرى أن: " لا تفعلوا ذلك بحقنا لأننا نستطيع أن نفعل نفس الشيء بكم"[3] مؤكدا على قدرة الولايات المتحدة على شن هجمات مضادة، و هو الأمر الذي لم يحدث فعليا فتواصل الاتهامات الأمريكية تزامن مع عدم اتخاذ تدابير فعلية مما أنبأ عن فشل الهجمات الأمريكية المضادة و عجز الردع السبيراني الأمريكي، و إلا و حسب الملاحظين لما توانت الإدارة الأمريكية بالتباهي بدفاعاتها السيبرانية ، و تؤكد هذه المؤشرات في الوقت نفسه قوة منظومة المعلومات الروسية، إذ يعتقد المحللون الإستراتيجيون أن الولايات المتحدة

---

[1] - "الاستثمار الالكتروني "،حديث العالم(2015)،آخر تحديث28 جانفي 2015
http://www.c4wr.com/الاستثمار- الالكتروني-وفوائده/

[2] - عادل عبد الصادق، "عسكرة الفضاء الإلكتروني "، مرجع سابق

[3] - "هل بإمكان الولايات المتحدة الأمريكية الانتصار في حرب الكترونية ضد روسيا ضد روسيا"، واشنطن بوست،(2016)،آخر تحديث 18 ديسمبر 2018
Katehon.com /article /hl-bmkn-lwlyt-Imthd-intsr-fy –hrb-lktrwny-did-rwsy

قامت بشن هجمات فاشلة عقب إصطدامها بأنظمة حماية معلومات روسية متطورة للغاية،[1] و هو ما أكدته المصادر العسكرية في واشنطن و الناتو بأن روسيا توصلت لامتلاك قدرات رهيبة في إدارة الحرب الإلكترونية، حتى أن البعض قدرها بأنها تساوي مجموع الطاقات الغربية مجتمعة.

و رغم تكثف الحديث خلال النصف الثاني من عام 2017 عن نشوب حرب باردة بين القوتين الولايات المتحدة وروسيا تفوق خطرا تلك التي سادت بعد نهاية الحرب العالمية الثانية الأمريكية بينها و بين الإتحاد السوفيتي سابقا إلا أن هناك من يعتقد أن تأزم العلاقات بين البلدين هو توتر عابر بالنظر إلى أن الحديث عن حرب باردة غدا موضوعا مستهلكا يتجدد كل حين بالتوازي مع كل أزمة تظهر في الأفق بين واشنطن و موسكو.[2]

غير أنه لا يكمن الإنكار أن الطبيعة السيبرانية للصراع الدائر بين الدولتين تجعل من روسيا تمثل تهديدا وجوديا للولايات المتحدة الأمريكية ،و هو الأمر الذي يثبته إقرار الكونغرس في 27 جويلية و بأغلبية ساحقة مشروع قانون لفرض المزيد من العقوبات على روسيا على خلفية اتهاماتها بالتدخل في مسار الإنتخابات الرئاسية الأمريكية و التورط عسكريا في كرانيا.

وتستهدف العقوبات الإقتصادية ضد موسكو صناعات الدفاع و الإستخبارات و التعدين و الشحن و السكك الحديدية كما تفرض قيودا على التعامل مع البنوك و شركات الطاقة في روسيا.

و في حين تستمر روسيا في إنكارها التام للمزاعم الأمريكية بل ان الرئيس الروسي بوتين تحدث عن دعوته أكثر من مرة الادارة الأمريكية للتعاون في مجال مكافحة القرصنة الإلكترونية، تستمر الولايات المتحدة في تطبيقها لقانون العقوبات بحق موسكو سنوات 2014 و 2015 حتى آخر عقوبات نهاية عام 2016 يضاف إليها السماح بفرض عقوبات جديدة عن " النشاط الذي يقوض الأمن الإلكتروني لصالح الحكومة الروسية".[3]

---

[2] - عمر نجيب، "الحرب الباردة المتجددة بين روسيا و الولايات المتحدة"،مرجع سابق

.

[3] - مرجع سابق.

المطلب الثاني :نماذج التنافس الرقمي الروسي- الأمريكي

لقد شكلت العسكرة الرقمية الروسية- الأمريكية مظهرا آخر من مظاهر الصراع الدائر بين الولايات المتحدة الأمريكية و الروسية والذي أخذ هذه المرة الشكل الالكتروني معبرا في ذات الوقت عن تفوق روسي في المجال ترجمته الانتهاكات الروسية المتكررة للمصالح الأمريكية .

أولا:التدخل في الإنتخابات الأمريكية:

أشار مجمع الإستخبارات الأمريكية أن روسيا تدخلت و أثرت على نتائج الرئاسيات الأمريكية عام 2016 فقد بدا واضحا تفضيل القيادة الروسية للمرشح الجمهوري دونالد ترامب[1] على مرشحة الحزب الديمقراطي هيلاري كلنتون بعد أن أكدت مصادر عدة وقوف الرئيس الروسي فلاديمير بوتين شخصيا[2] وراء ذلك عبر الحاق الضرر بحملة كلينتون و إضعاف الرأي العام في العملية الديمقراطية الأمريكية. و قد ذكرت وزارة الدفاع الوطني أن وكالة الإستخبارات الأمريكية على ثقة تامة بأن الحكومة الروسية وقفت وراء علميات القرصنة و تبادل الرسائل الإلكترونية بقصد التدخل في سير العمليات الإنتخابية، كما قامت المخابرات الروسية (GRU) بإختراق خوادم اللجنة الوطنية الديمقراطية (DNC) و حساب البريد الإلكتروني الشخصي لمدير حملة كلنتون: جون بوديستا و إحالة محتوياتها إلى موقع ويكيلكس الذي قام بتسريبها فيما بعد.

و يواجه أشخاص مقربين من ترامب إتهامات جنائية من بينهم مستشار الأمن القومي الجنرال مايكل فلين، و قد خلصت التحقيقات بثبوت وقوع إجتماعات بين مقربين من ترامب و السفير الروسي في واشنطن ورئيس اكرانيا السابق المقرب من موسكو.

و قد أعلن الرئيس السابق للولايات المتحدة الأمريكية باراك أوباما عن مواجهته شخصيا لبوتين و مطالبته له بالتوقف حالا عن تدخلاته في الشؤون الأمريكية، إلا أن المسؤولين الروس يستمرون في نفي أي تورط لهم في المسألة رغم شهادة مدير المخابرات الوطنية الأمريكية بوجود أدلة شرعية تثبت بأن عملية الإختراق (PNC) مرتبطة بعمليات روسية معروفة و أن روسيا تدخلت كذلك من خلال نشر الأخبار المزيفة و الشائعات المغرضة التي تم الترويج لها على وسائل التواصل الإجتماعي و لا تزال لحد الآن أزمة الإدعاء بالتدخل الروسي في الانتخابات الأمريكية تلقي بظلالها على الساحة الأمريكية. بعد أن أبدى الرئيس الأمريكي دونالد ترامب إستعداده للخضوع للإستجواب تحت القسم أمام المحقق الخاص روبرت مولر[3] بخصوص تواطؤ محتمل بين فريق حملته الإنتخابية و النظام الروسي خاصة بعد أن أخضع القضاء وزير العدل جيف سيشنز

---

[1]-"Y aura –t-il une cyberguerre froide entre les Etats Units et la Russie " ,RMC(2016)diffusion le 16 décembre 2016
RMC.bFmtv.com/emission/y-aura-t-il-unecyber-guerrefroide-entre-lesétats-unis-et-la-russie-1072089.html.

2-“ Piratage :la guerre froide numérique a commence ,Ouest france (2016), modifié le 16 Décembre 2016 russe riposte US
https://www.ouest-france.fr/monde/piratage-russe-riposte-us-la-guerre-froide-numerique-commence-468517

3-"التدخل الروسي في انتخابات الولايات المتحدة الأمريكية "،موسوعة ويكيبيديا (2018)،آخر تحديث،03 ماي 2018
التدخل –الروسي- في –إنتخابات- الولايات- المتحدة- الأمريكية https :lar.wikipedia.org/wiki/2016

[3] - محمد فوزي ،"التدخل الروسي في الانتخابات الأمريكية "العالم(2018)،آخر تحديث 25 جانفي2018
https://elbadil.com/2018/01/التدخل-الروسي-في-الانتخابات-الأمريكي

للاستجواب و لا تزال التحقيقات جارية بعد أن ثبت دس عملاء روس وسط الجماهير الأمريكية و إنشائهم لحساب مزيفة[1] على مواقع التواصل الاجتماعي بعد أن صرحت شركة فايسبوك[2] بأن ربع الإعلانات الروسية و التي بلغ عددها ثلاثة آلاف إعلان استهدفت مواقع جغرافية معينة في أمريكا، كما كشفت شبكة CNN أن عددا من الإعلانات المدعومة من قبل روسيا على موقع فيسبوك استهدف ولايات أمريكية لعبت دورا بارزا في فوز الرئيس الحالي بالانتخابات تتصدرها ولاية ميتشجان و ويسكنسون الأمريكيتان.[3]

ثانيا: قضية كاسبرسكي:

واجهت شركة "كاسبرسكي لاب" للأمن المعلوماتي عدة اتهامات من المسؤولين الأمريكيين تتلخص في كونها ربما تكون عرضة لنفوذ الحكومة الروسية. و قد جاءت الإتهامات اثر طلب لجنة الكونغرس الأمريكي المتكونة من 22 وكالة حكومية تزويدها بوثائق عن شركة كاسبرسكي باعتبار أن منتجات هذه الشركة يمكن أن تستخدم "لتنفيذ أنشطة شريرة ضد الولايات المتحدة".

و ذلك بعد أن تم تحذير الحكومة الأمريكية من طرف إسرائيل من إمكانية استخدام برمجيات كاسبرسكي الأمنية للتجسس على الولايات المتحدة.

و تحتسل شركة كاسبرسكي لاب لأمن المعلومات المركز الرابع عالميا بمجال حلول أمن المعلومات و لها فروع كثيرة في الولايات المتحدة و العالم أجمع ،و قد كانت إسرائيل هي من تفطنت لاحتواء برامج كاسبرسكي الأمنية على ثغرات تسمح باستخدامها كأدوات تجسس، و رغم نفي كاسبرسكي للتهم الموجهة إليها و لأي تنسيق مع الحكومة الروسية و إصرارها على التعاون مع المحقيين الفدراليين،[4] إلا أن وزير الأمن الداخلي للولايات المتحدة ألن ديوك كان قد وضع خطة لوقف استخدام منتجات الشركة في غضون 90 يوما مع فرض حظر على استخدام منتجاتها من قبل الأجهزة الحكومية. و عمدت كاسبرسكي لمقاضاة الحكومة الأمريكية و رفع دعوى لإلغاء الحظر الذي فرضته إدارة ترامب كون أن الخطوة أضرت بسمعتها التجارية و مصالحها دون أن تتوفر للحكومة أدلة قطعية بشأن المخالفات.

---

[1] -"شاهد كيف حدث التدخل الروسي المزعوم في الإنتخابات الأمريكية " ، CNN (2018)، آخر تحديث18 فيفري 2018 https:/arabiccnncom/world /wd-uselections-meddling-how-russia-did-it

[2]- " هكذا تدخلت روسيا في الإنتخابات الأمريكية"، صحيفة عاجل، قناةCNN (2017)،آخر تحديث04 أكتوبر 2017 .HTTPS///aje/sa/international/1955851

[3] - "عاجل"،مرجع سابق

[4] -"كاسبرسكي لاب يرفض إتهامات امريكا بالتجسس"،جريدة المال (2017)،آخر تحديث 16 أفريل 2018. كاسبرسكي- لاب- يرفض- إتهامات- امريكا- بالتجسس/http://www.almalnews.com/Story/372602/17

و تزعم إسرائيل أنها إخترقت شركة كاسبرسكي عام 2015 و توصلت إلى أن برامج مكافحة الفيروسات التي تعدها الشركة المذكورة آنفا ساعدت القراصنة الروس في التجسس على وكالة الأمن القومي .

و قد انفجرت القضية إثر قيام أحد موظفي وكالة NSA بنسخ معلومات غاية في السرية على محرك أقراص قابل للإزالة و اصطحابه معه للمنزل و تشغيله على كمبيوتره الشخصي المثبت عليه تطبيق مكافح الفيروسات كاسبرسكي و تمكنت روسيا من الوصول للملفات السرية و التي يحتمل أن تكون نوعا من الأسلحة الإلكترونية التي أحضرها الموظف لمنزله بغرض العمل عليها[1].

و رغم عدم توفر دليل يثبت تورط شركة كاسبرسكي في عملية التجسس إلا أنه تم التفطن إلى أن حل "Kasperskey-antivirus " يقوم بجمع البيانات المخزنة على أجهزة كمبيوتر المستخدمين و هو ما أثبت الشكوك الأمريكية بشأن كيفية توصل جهاز الأمن الفدرالي الروسي للملفات المنسوخة.

و قد رد يوجين كاسبرسكي رئيس الشركة على اتهامات وكالة الأمن القومي والموساد بأن الشركة وقعت ضحية منافسة أمريكية تحاول استبعادها من سوق الأمن المعلوماتي الرائجة ،فقد كان لقرار حذف منتجاتها أبعاد سياسية و أخرى اقتصادية بهدف طردها من السوق الأمريكية التي تستحوذ على 25 % من حجم أعمال الشركة فضلا عن زعزعة استثماراتها في جميع أنحاء العالم .

و يعد تطبيق كاسبرسكي من أفضل تطبيقات مكافحة الفيروسات في العالم[2]، يستخدم من قبل 400 مليون مستخدم فيما تؤكد ادارة الشركة سعيها لتحقيق الأمن المعلوماتي و مساعدة الحكومات أيا كانت جنسيتها في التصدي لمخاطر الانترنت ، رغم أنه وفي آخر تطورات الوضع أشارت وسائل الإعلام لتأكيد عدة وكالات حكومية أمنية ثبوت عمل شركة كاسبرسكي لدى المخابرات الروسية.

المطلب الثالث :معالم ميزان قوى جديد

إن نزوع موسكو لتحدي محاولات الولايات المتحدة الأمريكية فرض سيطرتها على مختلف دول العالم يمر عبر إسفزازات تتخذ من الهجمات الإلكترونية وسيلة لها و ذلك سعيا منها لترسيخ مكانتها على الساحة الدولية و هي في مجملها التطورات التي ظهرت للعيان كملامح حرب رقمية باردة منبأة في الوقت نفسه عن إرتسام ميزان قوى جديد تصوغه عوامل شتى كتشديد الخطاب و الإتهامات المتبادلة مع سوء التفاهم الذي ساهم في تأجيج الوضع بين الدولتين.

1- "كاسبرسكي ترد على إتهامات وكالة الأمن القومي و الموساد"، مرصد صحح خبرك(2017.)،آخر تحديث 20 أكتوبر 2017
www.shehkhabarak.com/NewsDetails.aspx ?id=3430

2-" الحكومة الأمريكية تحظر برنامج كاسبرسكي بسبب مخاطر التجسس"،(2017)، آخر تحديث 14سبتمبر2014
https://www.albraby.co.uk/medannews/2017/09/14

و قد أعلن فلاديمير أفيسيف مدير مركز الدراسات السياسية في موسكو " أنه لم تعد هناك مواجهة عسكرية مثل تلك التي وقعت بين حلف شمالي الأطلسي و حلف وارسو، اليوم لا روسيا و لا الغرب مستعدان لهجمات كبرى" كما أضاف " لم تعد هناك مواجهات عقائدية هناك خلافات"[1].

و يبقى الصراع على النفوذ قائما على المستويين العالمي و الإقليمي.

فروسيا التي إنتقلت إلى جهة رافضة في عدد من الملفات الدولية الحساسة بدءا من أكرانيا وصولا إلى الأزمة الروسية مرده رغبتها الكبيرة لاقرار ترسيم جديد للحدود الدولية و لو بالقوة، لذا تعمل على زعزعة الإستقرار في غرب البلقان بتقويض الديمقراطيات الحديثة و تقسيم المنطقة بنية فصلها عن بقية أوربا حتى تمنع السيطرة الغربية عليها، و بنية زعزعة إستقرار جنوب أوروبا كاشفة بذلك عن عقلية الحرب الباردة.

وفي حين "تتلكأ" الولايات المتحدة وراء دول صغرى مثل إسرائيل و السويد و فنلندا على مستوى الاستعداد للحرب الإلكترونية" في الوقت الذي يجري فيه سباق التسلح بلا هوادة في مضمار الحرب الإلكترونية .

و يظهر قراصنة الكمبيوتر الروس إهتمامهم الخاص بالطاقة[2] في الولايات المتحدة الأمر الذي بات يشكل أرقا لدى الأوساط الأمريكية ، رغم عدم إظهار الروس للمستوى المتطور من البرمجيات الخبيثة كالتي أظهرتها الولايات المتحدة عندما صممت برنامج ستوكسنت إلا أن الهاكرز الروس لديهم القدرة على إحداث إنقطاعات كبيرة في الولايات أمريكا خاصة فيما يخص أنظمة التحكم الصناعية كالماء و الغاز.

وحسب شركة سيمانتيك للأمن السيبيراني فوتيرة الهجمات التي تسارعت منذ سنة 2015 تعلن عن كم كبير من العدوانية، كما تؤكد ذات المصادر أن مطلقها مجموعة من القراصنة تعمل تحت إشراف و رعاية الدولة إذ أظهر الفاعلون براعة كبيرة بتحكمهم في تكاليف الطاقة لشركة الطاقة فضلا عن تحكمهم بالمعدات عن بعد مثل قواطع الكهرباء، وهو ما يعني أن تهديد إمدادات الطاقة أضحى شيئا في متناولهم. و يمكن لهجوم مماثل على شركة الكهرباء الأمريكية أن يتسبب في تأثيرات إقتصادية هامة إذ يرجح أن تبلغ الخسائر 1 ترليون دولار و حوالي 771 مليار دولار من متطلبات التأمين. وهو ما حول التعامل مع الهجمات الإلكترونية من مشكلة تكنولوجية إلى التعامل معها كمشكلة عسكرية

من جهته فقد أعلن الكرملين في تغريدة له على تويتر أنه يتفق مع قول الرئيس الأمريكي دونالد ترامب أن علاقات واشنطن "مع روسيا عند مستوى خطر للغاية هو الادنى على الاطلاق"[3].

و أضاف الناطق باسم الكرملين ديميتري بيسكوف أن الخطر يكمن في العجز عن التواصل و التعاون في المسائل شديدة الأهمية للبلدين و الشعبين .

---

[1] - عمر نجيب، مرجع سابق.

[2]-Ibid, Nakashima, R ussia has developped a cyberweapon “

[3] - عمر نجيب،"الحرب الباردة المتجددة بين روسيا والولايات المتحدة "،مرجع سابق

وفي حين توصف العقوبات الأمريكية على روسيا بأنها أكثر من شائكة على حد تعبير وزير الخارجية الألماني زيغمار غابربيال فان الحديث عن تهدئة محتملة للنزاع الرقمي الدائر يعد سابقا لأوانه بما أن الولايات المتحدة لايبدو أنها تعدل عن "الفظاظة " التي وسمت تعاملاتها مع القوة الروسية التي يديرها رجل مهووس بعظمة روسيا [1]المنبعثة مجددا عبر الوسائل الرقمية المتاحة.

خاتمة

كثيرة هي التحديات التي تواجه عالمنا اليوم والتي تفرضها بالأخص عدم امكانية السيطرة على التطبيقات العسكرية للفضاء السيبراني بعد أن غدت أدوات العسكرة الرقمية متاحة لكافة الفواعل الدولية و غير الدولية بشكل ساهم في تشكيل علاقات أكثر تشابكا بينها كتوفير الدول الدعم و الحماية اللازمين

[1] -مرجع سابق

لمجموعات مختلفة ......لتتولى تنفيذ العمليات السيبرانية الهجومية بحيث تتعدى الغاية من السيطرة على المؤسسات الى السيطرة على أنظمة بكاملها، وعليه نصل إلى الإستنتاجات التالية:

- ان توجه الدول نحو العسكرة الرقمية وما صاحبه من انتشار للأعمال العدائية في جميع أنحاء العالم والتي تقودها فواعل مختلفة أجج سباق التسلح الرقمي الجاري بلا هوادة، يجدربه تسليط الضوء على ضعف تكنلوجيا المعلومات والاتصالات على جميع المستويات وهو الضعف الذي نحدده بالهشاشة، هشاشة تجعل من السيطرة الفعالة على أمن الانترنت مسألة بعيدة المنال في الوقت الحالي نظرا للصعوبات السياسية و التشريعية و التقنية الكبيرة التي تواجهها في ظل عدم امكانية التحكم أو التنبؤ بسلوك الافراد الذين أضحوا فاعلين استراتيجيين في الفضاء الرقمي وتزيد التحديات تصاعدا في ظل احتمالية أن تفيض الحروب السيبرانية القائمة الى حروب كلاسيكية ضارية أمام عدم قدرة العالم على وقف نزيف المال و المعلومات و عدم استطاعة مبادئ الحماية الدولية مجاراة السرعة المتزايدة لاتجاه هذه النزاعات الجارية بلا توقف نحو الأساليب الهجومية .كما أن فتح الباب أمام رقمنة المنشآت الحيوية في ظل تكالب الدول على اعتماد الأنظمة الالكترونية كشكل من أشكال التحاقها بالركب الحضاري التكنلوجي شكل في ذات الوقت اضعافا لبنيتها التحتية الحساسة والتي غدت عرضة للتهديد المباشر . وفي ظل عدم جدوى الردع التقليدي لمقاومة طبيعة هذا التهديد المتغير و المتطور والمتجدد باستمرار فان العسكرة الرقمية وما يذكي نارها من سباق التسلح السيبراني الدؤوب، تتسارع الخطى نحو حرب عالمية ثالثة تنبئ بدمار يخترق الأذهان،و كما أن الوقوف موقف المتفرج يقود تماما للتهلكة مما يستلزم ادراك طبيعة التهديد وفهم تغيرات قواعد اللعبة الدولية و استيعاب أساليب العسكرة الالكتروونية الحديثة للعمل على ايجاد ضوابط و آليات تحد من هذا النشاط المهدد للجنس البشري .

فضلا عن أن تحول العالم الافتراضي الى عالم مشحون بالعدائية يهدد بتفجير كوارث واقعية خطيرة في ظل التطور الموازي في التحكم الآلي للعتاد الحربي الذي تكفي ضغطة زر هنا أو هناك في احداث أضرار لا حصر لها

- نجحت العسكرة الرقمية في تحويل قضايا الفضاء الافتراضي من قضايا سياسة دنيا الى قضايا مصنفة ضمن السياسات العليا بما يعني تحول الممارسات اليومية الى أعمال عسكرية خطرة وهو الذي يدعو للتساؤل عن ماهية الأطر المستخدمة للتعامل مع تلك الممارسات و ضبطها و كيفية تحديد المعايير التي يمكن الاعتماد عليها

وفي محاولة منا لاستشفاف أوجه تأثيرات السياسات السيبرانية الصاعدة في العلاقات الدولية و البدائل المحتملة لهذا التأثير نتساءل عن امكانية تبني أسس نظرية موضوعية جديدة نابعة من القضايا التي بات يطرحها الفضاء الرقمي،وهو التوجه الذي يبدو أكثر من ضروري خاصة:

- أن العسكرة الرقمية تشكل تحديا آخر من التحديات التي يواجهها كبار منظري العلاقات الدولية بما أنه لا نار ولا دخان للسلاح الرقمي فان الخطر أضحى قاب قوسين أو أدنى أمام المد المعلوماتي الجارف والذي عرفت القوى العالمية الكبرى كيفية بلورته في الاستثمارات الالكترونية التي جعلت من الطاقة الذكية عصب العالم الحديث يظل العالم الثالث الاكثر عرضة للخطر كونه أكبر مستهلك للتكنلوجيا الجاهزة و للأنظمة و البرامج المعلوماتية المعلبة ففي الوقت

الذي تباشر الدول باتخاذ التدابير الوقائية و امتلاك القدرات الالكترونية ، يقف العالم ليعلن عدم امكانية الانسحاب من العصر التكنلوجي فالاستعدادات تجري بلا توقف بغرض تبني العسكرة الرقمية ضمن الاستراتيجيات الوطنية و الأمنية للدول معلنة عن الاقرار بحرب المعلومات باعتبارها حربا للمستقبل مع عدم التوصل لامكانية ولو معقولة لصياغة اتفاقية دولية تسمح بتأطيرها ضمن قواعد القانون الدولي العام وهو الأمر الذي يرسخ لميزة التفوق فمن يحدد مصير المعارك المستقبلية ليس من يملك القوة فحسب بل القدر على شلها أيضا .

- ان اجتراح الفضاء السيبراني لميدان الصراع الدولي يقوض من المساعي الحثيثة لنشر الأمن و الاستقرار الدوليين ،لذا فالعسكرة الرقمية تتطلب استراتيجية مرنة تتوائم مع المتغيرات المستمرة الحاصلة على صعيد الفضاء السيبراني بغية مواجهة التهديدات الدولية المطروحة ، فهل يمكننا الحديث في نزاعاتنا المستقبلية عن حروب نزيهة و فوز مشرف في ظل عدم امكانية تمييز العدو عن الصديق .
- ان ثنائية تحول الفضاء السيبراني لعنصر حيوي لدعم وتحقيق الأهداف الاستراتيجية للفواعل الدولية وكمنفذ لوجيستي حاضن لنشاطاتها الاعلامية في مختلف مناطق العالم جعل من الأمن الدولي في حالة تعرض دائمة للخطر يعكسه سعي الدول المستمر للحصول على ميزات تنافسية جديدة على أعداءها مما يزيد في تفاقم الأخطار في ظل الجهل التام عن كيفية التعامل مع المتجددات الالكترونية على الساحة الدولية .
- إن الافتقار لأسس قانونية كافية لتبرير شن هجمات مضادة مع عدم كفاية الاشراف على الأذرع الحكومية المتعددة المعنية بالأمن الرقمي تظل مسألة العسكرة الرقمية معضلة حقيقية تذكي نار التوتر الدولي و تعمل بلا شك على التطور السريع لنظام دولي أكثر فوضوية محكوم بمبادئ غير واضحة المعالم تكبل جهود احلال السلام و الأمن الدولي في محيط دولي رقمي ذو خرائط حدودية مائعة تكاد تستحيل فيه فك خيوط ترابطاته المتشابكة مع كل ما يسجل من قصورفي كشف مصادر التهديد وسهولة و سرعة الاستهدافتتحول بذلك النزاعات الضيقة لصراعات طويلة الأمد.

وقد ارتأينا عدم الخوض في آفاق و مستقبل العسكرة الرقمية واء من الجانب النظري أو الجانب التطبيقي بسبب الحراك غير العادي الذي يتسم به المجال ،حتى أن الحكومات لا تزال تفكر في طريقة منطقية عن كيفية دمجها في الاستراتيجيات الوطنية الكبرى ففي حين تتخذها روسيا و عدد من الدول الأوروبية كآلية أساسية للدفاع الوطني ،تميل الولايات المتحدة الأمريكية الى اعتبارها سلاحا معاونا في حين ينصب تركيزها الأكبر على السلاح التقليدي والنووي بشكل أخص فرغم اظهارها للتقدم الكبير في مجال البرمجيات الالكترونية الا أن التفوق الرقمي لايكون دون التحكم في جميع موارد ومصادر العسكرة الرقمية

أن استحالة وضع قواعد خاصة بالرد في حالة النزاع الرقمي أمر ضاعف من صعوبة التعامل مع التهديدات المستحدثة التي تطرحها العسكرة الرقمية خاصة في ظل افتقار صناع القرار و السياسيون عموما للدراية التكنلوجية اللازمة و الراجعة أساسا لجهلهم بالحقل .

فعدم امكانية ترجيح أي سيناريو أو تنبؤ يرجع للحالة المتقلبة التي تتسم بها الأوضاع على صعيد الفضاء الالكتروني و التي تتميز بالتوتر و عدم الاستقرار بعدما أصبح بوسع أي كان اطلاق حرب سيبرانية

بسرعة بحبث يتم فرض الحرب على بلد بطريقة بقع فيها اللوم على بلد آخرمما يتسبب في مزيد من التصعيد بين تلك البلدان وينذر بالخطر الذي تتضاعف احتمالية وصوله للمستوى النووي .

ورغم كل ما سبق فانه لايسعنا الا الاقرار أن مرحلة السلام الالكتروني النسبي الهشة التي يعيشها العالم اليوم و التي لم تسفر عن اعتداءات سافرة على البنى التحتية خلال السنة الأخيرة ليست سوى استقرار نسبي مؤقت تكمن خلفه تهديدات شتى بحكم الأمور الكثيرة غير المرئية التي تحدث في عالم الانترنت .

فهرس الهوامش:

قائمة المراجع باللغة العربية:

كتب الكترونية :

- خليفة ،ايهاب." القوة الالكترونية وأبعاد التحول في خصائص القوة".
الإسكندرية،وحدةالدراسات المستقبلية،(2014). اطلع عليه بتاريخ08 فيفري2018.
https://www.bibalex.org/Attachments/PublicationslFile/2014070311292451794-awark12pdf.pdf

- جوزيف س.القوة الناعمة وسيلة النجاح في السياسة الدولية، تر د. محمد توفيق البجيرمي .
السعودية:العبيكان ،الطبعة العربية الأولى، 2007 . اطلع عليه بتاريخ12فيفري2018
-جوزيف - - pdfhttps://www.scribd.com/document/366354634/

- عبد الصادق، عادل. "الارهاب الالكتروني و القوة في العلاقات الدولية نمط جديد وتحديات مختلفة".مصر : مركز الدراسات السياسية و الاستراتيجية، 2009 . اطلع عليه بتاريخ 27 فيفري 2018
http://accronline.com/book_detail.aspx?id=75

- ." الحرب الالكترونية : ."
الالكترونية (بيروت ،الطبعة الأولى ،2010).

- الفتلاوي ،أحمد عبيس ."الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر".(: 2015) 614-61
:

-ناي ،جوزيف الابن ."المنازعات الدولية ".ترأحمد أمين الجمل ومجدي كامل . : الجمعية المصرية لنشر المعرفة و الثقافة العالمية ،الطبعة العربية الأولى ،1997

قالات في مواقع و دوريات الكترونية:

- . "القوة الالكترونية : ."
مؤتمر حروب الفضاء السيبيراني.(2012)اطلع عليه بتاريخ 06 فيفري 2018.
http://www.accronline.com/article_detail.aspx?id=4747 -

- . "استخدام القوة الالكترونية في التفاعلات الدولية الجزء
المعهد المصري للدراسات،(2015).اطلع عليه بتاريخ04 فيفري 2018."
— — الدولية — — الالكترونية — — / .-org.eg https://eipss
/

- . "استخدام القوة الالكترونية في التفاعلات الدولية الجزء
المعهد المصري للدراسات (2016).آخر تحديث 19 2016."
—الدولية — — الالكترونية — - / https://eipss-eg.org/

- ." : بين التحديات و فرص المواجهة".
اطلع عليه بتاريخ16 فيفري 2018.

[1] (http ://www.accronline.com/article_detail.aspx ?id=28402

- "أنماط الحرب السيبيرانية وتداعياتها على الأمن العالمي"،مجلة السياسة الدولية (2017) أطلع عليه بتاريخ 26فيفري 2018 http://www.siyassa.org.eg/News/12072.aspx
- الياسري، ."الفواعل من غير الدول في العلاقات الدولية". 4802 (2015).
- http://www.ahewar.org/debat/show.art.asp?aid=4673
- عبد الرحيم، عزت . كيف سيطر الجيش الاسرائيلي على مواقع التواصل الاجتماعي ، مقدمة للعسكرة الرقمية ،لايدي كونتسمان و ريبيكا ستاين : الدراسات الاستراتيجية،13جويلية 2015،،اطلع عليه بتاريخ 16 فيفري2018 http://rawabetcenter.com/archives/9492
- الحياري،ايمان."مفهوم الحرب الالكترونية" . (2016).آخر تحديث 22 ديسمبر 2016 [1]
مفهوم - الالكترونية/http://mawdoo3.com-
-- "ما هي السيبرانية ؟ و ما هو دورها في صناعة القرار".زايتجايست و مشروع فينوس(2012).آخر تعديل26 ديسمبر 2012.
- العباسي، ريهام عبد الرحمان رشاد ."أثر الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية ،دراسة حالة :تنظيم الدولة الاسلامية".المركز الديموقراطي الـ (2016) .آخر تحديث 24 جويلية 2016.
https://democraticac.de/?p=34528
- "الحروب السيبرانية :تصاعد القدرات و التحديات للأمن العالمي " . (2017).آخر تحديث12 2017
http://accronline.com/article_detail.aspx?id=28395
- " أسلحة حرب المعلومات و استخداماتها".أرشيف إسلام أون لاين .اطلع عليه في 04 ماي 2018، 00https://archive.islamonline.net/?p=982.
-شفيق، نوران ."أثر التهديدات الالكترونية على العلاقات الدولية:دراسة في أبعاد الأمن الالكتروني ".المكتب العربي للمعارف.اطلع عليه بتاريخ15 أفريل2018.
https://books.google.dz/books?id=r7dQDwAAQBAJ&pg=PP1&lpg=PP1&dqsource=bl&ots=ZuS6WuCNMs&sig=9tuly7onRweyQOerdZD0tk0Cd
-" هل تعرف معنى "ويكيليكس ولماذا يعيش مؤسسه في سفارة منذ 4 أعوام".ملفات ويكيليكس و بنما السرية(113) . سبوتنيك(2016).آخر تحديث 02 أكتوبر 2016.
https://arabic.sputniknews.com/art/201610021020317067-ويكيليكس/ –أسانج – وثائق –تسريب
-"تسريبات سنودن الأخطر في تاريخ أميركا".سكاي نيوز عربية (2013).آخر تعديل26 أكتوبر 26.10.2013.
تسريبات – سنودن– الاخطر– في – تاريخ – أمريكا
https://www..skynewsarabia.com/461551

أدمام ،شهرزاد." الفواعل العنيفة من غير الدول :دراسة في الأطر المفاهيمية و النظرية".المنهل.
سياسات عربية ،العدد الثامن مارس (2014)
اطلع عليه بتاريخ30 أفريل 2018
https://platform.almanhal.com/Files/2/50789

- بن يوسف،نبيلة. "مستقبل العلاقات الدولية في ظل وجود فواعل جديدة ..المنظمات العالمية غير الحكومية " " ballni.kadem@yahoo.fr". آخر تحديث 21 2012
http://kenanaonline.com/users/nabilabenyoucef/posts/463015

-"السيبرنيتيك أو القيادة الذاتية الهاددفة عن طريق مكننة الفكر"
www.albadr.org/www/doc/sitevisitors/3.d

- منى،زياد ."العسكرة الرقمية ". (2015).اطلع عليه بتاريخ03 2018
http://www.aranthropos.com/

[1] - Militarisme ,wikipedia(2018), dernière modification le 13 juin 2018
https://fr.wikipedia.org/wiki/Militarisme

–البهي،رغدة ."الردع السيراني: المفهوم والاشكالية و المتطلبات". مجلة العلوم السياسية و القانون العدد الأول .المركز العربي الديموقراطي(2017). آخر تحديث21 فيفري2017.
https://democraticac.de/?p=43837

-"هجماتdos لالكترونية" .الباحثون السوريون(2017) .آخر تحديث 02 2017 .
https://www.syr-res.com/article/14290.htm

– الشهيل، ليلى. " سيلفي عسكري"الجديد .العدد الرابع (2015).
http://www.aljadeedmagazine.com/?id=546

- خليفة ، ايهاب. " الكتائب الالكترونية الدول تفقد سيادتها في حروب مواقع التواصل الاجتماعي ".ملكية كركود(2016) .آخر تحديث 11 2016.
-www .france 24com /ar/20161111

- جعيجع ،عبد الوهاب جعيجع ." ادارة العلاقات الدولية ".الموسوعة الجزائرية للدراسات السياسية و الاستراتيجية (دار الخلدونية، الطبعة الأولى، 2016) .
تحديث01 2018
https://www.politics-dz.com/community/threads/almn-almylumati-u-dar-alylaqat-alduli.10851/

– باكير،علي حسين." المجال الخامس ... الحروب الالكترونية في القرن ال21".مركز الجزيرة للدراسات(2011).آخر تحديث 12 جانفي2011.
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

- "خطر الحروب السيبرانية عبر الفضاء الالكتروني".(2017).آخر تحديث سبتمبر 2017
http://aitmag.ahram.org.eg/News/83562.asp

-رشيد مهدي الياسري،م. "الارهاب الالكتروني وطرق مواجهته ". (2017).آخر تحديث 25 2017 .
http://fcdrs.com/polotics/766

-الفيل ،علي عدنان ." الارهاب الالكتروني ". .مجلة الجامعة الخليجية ، العدد الثاني (2010)
ttpsh://formplat.almanhal.com/files/2 /7983

- البنداري ،محمد مبارك. "الارهاب الالكتروني مفهومه ووسائل مكافحته".شبكة ضياء (2014).آخر تحديث 29أكتوبر 2014 ،
https://diae.net/16243

- "ما هي السيبرانية ؟ و ما هو دورها في صناعة القرار".زايتجايست و مشروع فينوس(2012). تعديل26 ديسمبر2012.
http://www.zeitgeistarabia.com/2012/12/cybernation.html

-البري ،يوسف عبد الغني حجاج ."نشأة وتطور حرب المعلومات ". مؤتمر حروب الفضاء السيبراني(2015).آخر تعديل 15 ماي 2015.
https://seconf.wordpress.com/2015/05/15/نشأة –و تطور – حرب –المعلومات

- كيشك ،محمود "الحرب الباردة ...السبب الأول في اختراع الانترنت". جورناس (2012).آخر تعديل 03 فيفري 2012.
Journas .com /–KoshkAlmady/post/44490/ الحرب–الباردة – السبب– الأول –في – اختراع – الانترنت

- "الحروب السيبرانية :تصاعد القدرات و التحديات للأمن العالمي " .
(2017).آخر تحديث12 2017.
http://accronline.com/article_detail.aspx?id=2839

- . " تغير مفاهيم القوة و التوازنات العالمية":
. (2017).
آخر تحديث 17 أفريل 2017
– – –تغير مفاهيم – –
- https://alarab.co.uk/العالمية

– " أسلحة حرب المعلومات و استخداماتها".أرشيف إسلام أون لاين اطلع عليه في 04 ماي 2018.
https://archive.islamonline.net/?p=982

– البري ،يوسف عبد الغني حجاج ."نشأة وتطور حرب المعلومات ". مؤتمر حروب الفضاء السيبراني(2015).آخر تعديل 15 ماي 2015.
https://seconf.wordpress.com/2015/05/15/نشأة –و تطور – حرب –المعلومات

- " أسلحة حرب المعلومات و استخداماتها".أرشيف إسلام أون لاين اطلع عليه في 04 ماي 2018.
https://archive.islamonline.net/?p=982

1- "هل تعرف معنى "ويكيليكس ولماذا يعيش مؤسسه في سفارة منذ 4 أعوام".ملفات ويكيليكس و بنما السرية(113) . سبوتنيك(2016).آخر تحديث 02 أكتوبر 2016.
https://arabic.sputniknews.com/art/201610021020317067-ويكيليكس/ –أسانج –
وثائق –تسريب

[1]-"تسريبات سنودن الأخطر في تاريخ أميركا".سكاي نيوز . (2013) .آخر تعديل26 أكتوبر 2013.
تسريبات – سنودن– الاخطر – في – تاريخ – أمريكا
https://www..skynewsarabia.com/461551

- حسني، اسراء ."أخطر وثائق سربها عميل الأمن القومي الأمريكي تكشف تجسس أمريكا على العالم تتبع هواتف رؤساء الدول ..اختراق أجهزة حكومية صينية ..الوصول الى مراكز بيانات جوجل ياهو..التنصت على الهواتف حتى المشفرة منها". اليوم السابع. آخر تعديل 06 أكتوبر 2015
أخطر –وثائق –سربها –عميل –الأمن – القومي–تكشف–
https://www.youm7.com/story/2015/10/23761096 /تجسس

-عبد العزيز ، "الحرب السيبرانية :التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية ".المنهل (2018). عليه بتاريخ 04 أفريل 2018.
https://platform.almanhal.com/Files/2/100742

- [1]- كركود ،مليكة.- " الكتائب الالكترونية الدول تفقد سيادتها في حروب مواقع التواصل الالكترونية- - - - 24com /ar/20161111 France 24." (2016) .آخر تحديث 11 2016 .
www .france

- ." هل تشكل مواقع التواصل الاجتماعي تهديدا للأمن القومي". السياسة الدولية(2015).آخر تحديث 07 2015.
http://www.siyassa.org.eg/News/15182/

- ت، يوسف ."أشهر عمليات التجسس الرقمية في الخمس سنوات الأخيرة" .طلائع الجزائريّن .مكتب الدراسات الاستراتيجية الأمنية .المرصد الجزائري(2017).آخر تحديث 27 مارس 2017.
http://marsadz.com/

1- أوشن، نصر الدين ."النظرية الليبيرالية في العلاقات الدولية".الجزائر : أم البواقي،جامعة العربي بن مهيدي

2- / 5510763 www.academia.edu/ -[1]

3- ديناميكيات الانتقال من الصلبة الى الناعمة الى الافتراضية ".السياسة الدولية محمود أبو ليلة: "
(2012). تحديث 14 أفريل 2012.

http://www.siyassa.org.eg/News/2376.aspx

- "ايشلون ..،..أذن الشيطان ..أو كيف تتجسس أمريكا على العالم".منتدى الجيش العربي(2013) آخر تحديث28 أكتوبر 2013.

http://www.arab-army.com/t84615-topic

- سامر مؤيد عبد اللطيف ". الرقمي رؤية مستقبلية ". مركز الدراسات القانونية و الدستورية. (2015)

https://www.iasj.net/iasj?func=fulltext&aId=104012

- طه ،غسان ." القوة الجاذبة وأساليب المواجهة ". (2015).آخر تحديث 09 جويلية 2015 . _ (_ _ _وأساليب_المواجهة)

http://softwar-lb.org/4338/296/

- فندي، سارة "النظرية البنائية في حقل العلاقات الدولية ". الموسوعة الجزائرية للدراسات السياسية و الاستراتيجية(2017).آخر تحديث 19 ديسمبر 2017

https://www.politics-dz.com/community/threads/alnzri-albnai-fi-xhql-alylaqat-alduli.10518

- مقدمة لتأثير السياسات الافتراضية الصاعدة في العلاقات الدولية لنازلي. السياسة الدولية (2013).آخر تحديث20 2013

http://www.siyassa.org.eg/News/3352.aspx

- "ما هو الأمن السيراني".المواطن(2017). آخر تحديث31 أكتوبر2017.

https://www.almowaten.net/2017/10

- "أشهر هاكرز على مستوى العالم ". (2014).آخر تحديث 08 2014.

/https://www.sasapost.com/hackers

- مجيد،عبد الاله ."سباق تسلح الكتروني حقيقة واقعة برأي غالبية ".ايلاف(2012). تحديث 01 فيفري2012.

http://elaph.com/Web/news/2012/2/713508.html .

- الاسدي، مروة ."سباق التجسس الالكتروني و زعزعة النظام العالمي".جريدة الاعلامي (2018). آخر تحديث 26 جانفي2018.

http://www.themediamagazine.com/ArticleDetail.aspx?id=9990

- "قوة الفضاء السيبراني: الثقافة و السياسة في الفضاء الالكتروني و الانترنت" pdf . على الرابط https://wwww.palitics-dz.com/theads/du تاريخ الاطلاع 21 فيفري

- مروة الاسدي" .سباق التسلح الالكتروني ". النبأ(2018) .

annabaa.org/Arabic/information/105-89

- "الحرب الالكترونية :عندما يصبح الحاسوب فتاكا".الجزيرة (2016). تحديث 16 2016.

- الزيداني، صلاح الدين أبو بكر . "طبول الحرب الرقمية". مجلة المسلح(2016).آخر تحديث 14 جانفي 2016. www.almusallh./y/ar/thoughhte
[1]--https://platform-almanhal.com/files
- حميدة، كريم."القرصنة الالكترونية". الألوكة الثقافية (2013).آخر تحديث 04 أفريل 2013 .
العالم بينهم مصري" (2017)،آخر تحديث30 ديسمبر 2015
http://www.soutalomma.com/Article/79284/
- 11أخطر هاكر في العالم بينهم مصري". (2017).
تحديث30 ديسمبر 2015.
http://www.soutalomma.com/Article/79284/
- مرعي،اسراء جبريل رشاد. "الجرائم الالكترونية: الأهداف- - طرق الجريمة و معالجتها".المركز الديموقراطي العربي للدراسات الاستراتيجية و الاقتصادية و السياسية(2016)،آخر تحديث 09 2016.
https://democraticac.de/?p=35426
- البنداري ، محمد مبارك ."الارهاب الالكتروني مفهومه ووسائل مكافحته"، شبكة ضياء (2014)،آخر تحديث 29أكتوبر 2014 .
.https://diae.net/16243
- الفيل ، علي عدنان. الارهاب الالكتروني ." مجلة الجامعة الخليجية . جامعة الموصل ،كلية الحقوق ،مجلة الجامعة الخليجية ،العدد الثاني(2010)
ttpsh://formplat.almanhal.com/files/2 /7983
- البداينة ،ذياب موسى."الارهاب المعلوماتي" .ورقة مقدمة للحلقة العلمي الارهاب. جامعة نايف العربية للعلوم الأمنية ، 15 -19 2008. اطلع عليه بتاريخ 16 أفريل 2018.
https://repository.nauss.edu.sa/bitstream/handle/123456789/56415
.pdf?sequence=1&isAllowed=y
- "الارهاب الالكتروني و طرق مواجهته " .شبكة النبأ المعلوماتية (2010)
https://annaba.org/arabic/informatics/11123
- اللواتي ،نسرين فوزي. " العامل الحاسم في مواجهة الخصوم". (2017). آخر تحديث 25
http://aitmag.ahram.org.eg/News/77865.aspx2017
- خليفة، ايهاب ."cyber pawer: التطبيقات الأمنية لقوة الفضاء الالكتروني". (2014). آخر تحديث16 201.
http://www.accronline.com/article_detail.aspx?id=1981
- "مخاوف أمريكية من هجمات الكترونية". الجزيرة . اطلع عليه بتاريخ 12 أفريل2018 .
www.ahjazira.net/programmes/
- " الجيش السوري الالكتروني".موسوعة ويكيبيديا(2018).آخر تحديث 29 2018.
https://ar.wikipedia.org/wiki/ الجيش_ _

- "الحرب الرقمية ومنظومة السيطرة الكاملة".مجلة الجيش(2003).آخر تحديث جويلية2003 .
-الرقمية- -السيطرة- https://www.lebarmy.gov.lb/ar/content/
- الياسري،م حوراء رشيد مهدي "الارهاب الالكتروني وطرق مواجهته ". (2017).آخر تحديث 25 2017
.http://fcdrs.com/polotics/766
- شفيق ، نوران. "أشكال التهديدات الالكترونية و مصادرها ". الارهاب و الاستخبارات(2017) .آخر تحديث 10 ديسمبر 2017.
https://www.europarabct.com/B1%D9%87
- غايب ، محروس نصار. "الجريمة المعلوماتية" .المعهد التقني الأنبار(2011). اطلع عليه بتاريخ05 ماي 2018.
https://www.iasj.net/iasj?func=fulltext&aId=28397
- العربي ،محمد مسعد ."من الدولة الى الفرد : تأثير السياسات الافتراضية الصاعدة في العلاقات الدولية ". السياسة الدولية(2013).آخر تحديث 20 نوفمبر 2013.
http://www.siyassa.org.eg/News/3352.aspx
- "ما هي أفضل خمسة جيوش الكترونية في العالم و ماترتيب الجيش السيبراني الروسي". KATEHO.(2017).آخر تحديث13جانفي2017.
http://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy
- "السلاح السيبراني أخطر من النووي" .صحيفة ايزفيستيا(2016). آخر تحديث29 أفريل2016.
https://arabic.rt.com/press/821142-السلاح-السيبراني-النووي
- ناي ، جوزيف س الابن." التحكم في الصراع السيبراني". مدونات الجزيرة(2017) . 09 أوت 2017
http://blogs.aljazeera.net/blogs/2017/8/9
- البهي، رغدة ." مخاطر سباق التسلح المعلوماتي في القرن الحادي و العشرين ". طومسون رويترز و المجلس الاطلسي. FUTURE(2017)01نوفمبر 2017.
https://futureuae.com/book.php/Mainpage/Item/3400/big-data
- ." تنازع الاختصاصات في الجرائم الالكترونية".) .(
https://dspace.univ-ouargla.dz/jspui/bitstream/123456789/7143/3/D0211.pdf

- بسيوني ،محمد. "عقيدة جيراسيموف : دوافع الإستراتيجية الروسية لحرب لمعلومات ضد الدول الغربية". الصباح الجديد. مركز المستقبل(2017).آخر تحديث 23 أكتوبر 2017.
- "الحرب الباردة مستعرة في الفضاء الالكتروني ". صحيفة العرب (2017). آخر تحديث 13أكتوبر 2017.

الحرب- الباردة- مستعرة- في- الفضاء- الالكتروني/ https://alarab.co.uk
- العزاوي ،مهند ."الاستراتيجية الأمريكية بين مزدوجي المهارشة و القدرة المكتسبة". العرب نيوز (2010) .آخر تحديث 20 أفريل 2010.

www.alarabnews.com/show2.asp?NewId=24995&PageId=12xPartId=1
- الهرمزي،سيف. "مقتربات القوة الذكية الأمريكية كآلية من آليات التغيير الدولي: الولات المتحدة نموذجا". المركز العربي للأبحاث و دراسة السياسات،الطبعة الأولى (2016).اطلع عليه بتاريخ 20 أفريل 2018 .

https://ia800605.us.archive.org/27/items/005VX/005VW00441.pdf
- "مصطلح القوة الذكية نهج جديد في السياة الخارجية الأمريكية خلال فترة أوباما " .
(2014).آخر تحديث 03 2014.
http://rawabetcenter.com/archives/977
- عبد الصادق ،عادل ."أمريكا و تشكيل قيادة عسكرية في الفضاء الإلكتروني: هل بدأ الإستعداد لحروب المستقبل ؟".مركز الأهرامات للدراسات ،السكينة(31.08.).آخر تحديث 31 أوت 2011
https://www.assakina.com/news1/9379,html
- "وزير الدفاع الأمريكي ليون بانيتا يحذر من هجمات الكترونية شديدة الخطورة قد تتعرض لها بلاده".الجزيرة (2012).آخر تحديث 15 أكتوبر 2015
- " مواجهة روسيا والصين في صلب استراتيجية البنتاغون الجديدة" . (2018) . آخر تحديث 19 جانفي2018.
- مواجهة-روسيا-والصين-في-صلب-استراتيجية-البنتاغون
https://arabic.rt.com/world/922151-
-"مخاوف أمريكية من هجمات إلكترونية" .الجزيرة(2012).آخر تحديث 10 أكتوبر 2012.

www.Aljazeera.net/program /bihind-thenews/2012/10/15/
- "البنتاغون يرفع مستوى ادارة الحرب الرقمية من سلاح معاون الى قيادة قتالية مشتركة ". اليوم السابع(2018).آخر تحديث 21 أفريل 2018.

https://www.youm7.com/story/2018/4/21/
- نجيب، عمر . "الحرب الباردة المتجددة بين روسيا و الولايات المتحدة: معالم ميزان قوى عالمي في طريق التشكل". رأي اليوم (2018).آخر تحديث 18 سبتمبر 2017.

https://www.raialyoum.com/index.php/- – -بين – روسيا – والولايات-
الأمريكي-

- ."استراتيجية المحاور الأربعة :الرئيس الأمريكي يعلن خطة جديدة للأمن
.. الصين وروسيا تعملان ضد مصالح الولايات المتحدة الأمريكية ..:
السابقون سبب ضعف واشنطن وتمدد ايران ". اليوم السابع (2017).آخر تحديث 19 ديسمبر 2017.

https://www.youm7.com/story/2017/12/19/

- الخالد، عمرو. "الأمن الالكتروني من أهم مرتكزات اقتصادات الطاقة الذكية ". البوابة العربية(2018).آخر تحديث 08 مارس 2018.

/ الأمن الالكتروني – أهم–مرتكزات–اقتصا_/2018/03/08 /https//aitnews.com

- هاشم، عزة "عسكرة الفضاء، الحروب السيبرانية، أمن الطاقة". مركز الدراسات الإستراتيجية و الدولية المتحدة (2016).آخر تحديث }جانفي 2016.

.https://futureae.com/ar/mariage/ttem/659/

- " ".حديث العالم(2015).آخر تحديث28 2015.

/ - - http://www.c4wr.com/

- "هل بإمكان الولايات المتحدة الأمريكية الانتصار في حرب الكترونية ضد روسيا ضد روسيا" واشنطن بوست(2016). آخر تحديث 18 ديسمبر 2018.

Katehon.com /article /hl–bmkn–lwlyt–lmthd–intsr–fy –hrb–lktrwny–did–rwsy

- "التدخل الروسي في انتخابات الولايات المتحدة الأمريكية ."موسوعة ويكيبيديا (2018).آخر تحديث03 ماي 2018.

التدخل –الروسي – في –إنتخابات– الولايات– المتحدة– الأمريكية
https :lar.wikipedia.org/wiki/2016

- فوزي ، محمد. "التدخل الروسي في الانتخابات الأمريكية" العالم(2018).آخر تحديث 25 جانفي2018.

https://elbadil.com/2018/01/التدخل–الروسي–في–الانتخابات–الأمريكي

- " هكذا تدخلت روسيا في الإنتخابات الأمريكية". صحيفة عاجل. قناةCNN (2017). آخر تحديث04 أكتوبر 2017.

.HTTPS///aje/sa/international/1955851

- "كاسبرسكي لاب يرفض إتهامات امريكا بالتجسس."جريدة المال (2017). آخر تحديث 16 أفريل 2018.

كاسبرسكي– لاب– يرفض– إتهامات– امريكا–
بالتجسس http://www.almalnews.com/Story/372602/17/

- "البنتاغون يرفع مستوى ادارة الحرب الرقمية من سلاح معاون الى قيادة قتالية مشتركة ". اليوم السابع(2018).آخر تحديث 21 أفريل 2018.

https://www.youm7.com/story/2018/4/21/

- "كاسبرسكي ترد على إتهامات وكالة الأمن القومي و الموساد".مرصد صحح خبرك(2017).آخر تحديث 20 أكتوبر 2017.

www.shehkhabarak.com/NewsDetails.aspx ?id=3430

- " الحكومة الأمريكية تحظر برنامج كاسبرسكي بسبب مخاطر التجسس"،(2017)، آخر تحديث 14سبتمبر 2014

https://www.albraby.co.uk/medannews/2017/09/14

وثائق رسمية :

- "دليل الأمن السيبراني للدول النامية ". (2006).
https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf
- فريق الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية . "
الجريمة السيبرانية والتدابير الي تتخذها الدول الاعضاء و المجتمع الدولي والقطاع الخاص للتصدي لها ". UNODC (2013).اطلع عليه28 أفريل2018.
https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_A.pdf

:

- عبد الفتاح، نبيل ."مقدمة للارهاب الالكتروني والقوة في العلاقات الدولية نمط جديد وتحديات " مركز الدراسات السياسية والاستراتيجية،2009.اطلع عليه بتاريخ
25 فيفري2018
http://accronline.com/book_detail.aspx ?id=75
- "السياسة السيبرانية في العلاقات الدولية"
السياسة الدولية،،2013آخر تحديث 20 2013

http://www.siyassa.org.eg/News/3352.aspx

أوراق مقدمة في ملتقيات و ندوات وطنية و دولية :

-قادير ،اسماعيل."ادارة الحرب النفسية في الفضاء الالكتروني :الاستراتيجية الامريكية الجديدة في . " ورقة مقدمة للندوة الدولية حول عولمة الاعلام- السياسي و تحديات الأمن القومي للدول النامية جامعة الجزائر3،كلية العلوم السياسية و العلاقات الدولية،
Ismail_enssp@yahoo.com

معاجم و قواميس الكترونية:.

- العسكرة،معجم الوسيط،قاموس المعاني ،اطلع عليه بتاريخ 03فيفري2018

/.   /   https://www.almaany.com/ar/dict/ar-ar

- عسكرة ،معجم الرائد،قاموس المعاني، اطلع عليه بتاريخ03فيفري2018 https://www.almaany.com/ar/dict/ar-ar/ ?c=

- لعسكرة ،معجم الغني ،قاموس المعاني الالكتروني،اطلع عليه بتاريخ 03فيفري2018
- ني ،قاموس المعاني الالكتروني،أطلع عليه بتاريخ 03 فيفري2018 https://www.almaany.com/ar/dict/ar-ar/

بحوث و رسائل تخرج جامعية :

- وارن سينغر، بيتر و فريدمان، ألن أ، " الأمن الالكتروني و الحرب الالكترونية". تر فخر الدين قاسم احمد، مجاهد . السودان: بحث تكميلي لنيل درجة الماجستير في الترجمة ، جامعة السودان للعلوم و التكنلوجيا : 18. اطلع عليه بتاريخ 02 مارس 2018.

Repository.sustech.edu/bitstrem/handle/123456789 /14861/66- الصفحات%20ترجمة%20281% .pdf?sequence=1&isAllowed=y

- الحانوتي ،تيسير ."امن المعلومات هاجس العالم الرقمي ".

https://drive.google.com/file/d/1I9KO11zLbRSawBuvFdPJaZoEXEWeJnj8/view

- طاجين، فريدة ."دور مجتمع المعلومات في تعزيز الأمن الانساني : دراسة حالة ماليزيا ". أطروحة مقدمة لنيل شهادة دوكتوراه العلوم في العلوم السياسية و العلاقات الدولية ، تخصص علاقات دولية ،جامعة بسكرة ،، 2015 –2016 .

http://aitmag.ahram.org.eg/News/83562.asp

موسوعات علمية:

- جاسوسية رقمية ".موسوعة ويكيبيديا (2018).آخر تحديث 31 2018.

https://ar.wikipedia.org/wiki/ جاسوسية –رقمية

- "حرب الانترنت" موسوعة ويكيبيديا الحرة (2018) .آخر تحديث 08 جانفي 2018.

https://ar.wikipedia.org/wiki/حرب الانترنت

- " ." موسوعة ويكيبيديا (2018).آخر تعديل 17 2018 .

https://ar.wikipedia.org/wiki /

- "الانونيموس".موسوعة ويكيبيديا(2018).آخر تعديل 20 2018.

(https://ar.wikipedia.org/wiki/ ونيموس-_)

- " ترونية :نشأتها وتطورها ومفهومها". أطلع عليه بتاريخ 13 . 2018.

http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec03.doc_cvt.html

قائمة المراجع باللغة الفرنسية:

Articles :

Center for *Security* ". Cyberguerre :concept,état d'avencement et limites" -
) 2010(Studies(CSS),ETH Zurich,N 71
*h*ttp://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-71-FR.pdf

Opération Tompora : comment les brétanniques dépassent les américains " -
.22 13 2013. LEXPRESS.fr(2013)."pour espionner Internet
https://lexpansion.lexpress.fr/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_1434134.html

Le système Echelon :une nouvelle donne dans l'espionnage électronique -"
institut québécois des hautes études internationales, (université ".
.LAYAL,bullettin N° 50 janvier 2001)
http://www.cms.fss.ulaval.ca/recherche/upload/hei/fichiers/bulletin50.pdf

." La guerre numérique"Hermans ,Michel. -
, " Michel.Hermans@ulg.ac.be
https://orbi.uliege.be/bitstream/2268/168643/1/La%20guerre%20num%C3%A9rique.pdf

, Le québécois libre, vu le "les fendement du libéralisme"- Ludwig Von Mises,
03mai2018
http://www.quebecoislibre.org/08/080120-2.htm

ASPJ " La cyber-dissuasion est-elle une stratégie illusoire ?."IasiEllo, Emili. -
Afrique & Francophonie , 1er trimestre(2018).
http://www.airuniversity.af.mil/Portals/10/ASPJ_French/journals_F/Volume-09_Issue-1/iasiello_f.pdf

20 ". russie re cybernétique contre larse prépare à une gue L'otan – "
octobre 2012.
https://www.alterinfo.net/L-OTAN-prepare-une-guerre-cybernetique-contre-la-Russie_a82691.html

Comment le gouvernement russe se prépare la cyberguerre à " -
Mediapart(2017).modifié le 31 juillet2017.."veunir ?
https://blogs.mediapart.fr/grandfach-xcom/blog/290717/enquete-comment-le-gouvernement-russe-se-prepare-la-cyberguerre-venir

.Yandex States(2017).modifié le "La Russie crée une armée cybernétique – "
24 fevrier 2017.

https://infosdanyfr.wordpress.com/2017/02/24/la-russie-cree-une-armee-cybernetique/

rre eUkraine,veritable laboratoire de la gu " Sébastien.,obertG -
cybernétique", les voix du monde RFI(2017).modifié le 11 octobre 2017
ukraine-veritable-laboratoire-gurre-cybernetique-www.rfi.fr/emission/2017

.wikipédia(2018). modifié le 02 juin 2018."La cyberguerre "-
https://fr.wikipedia.org/wiki/Cyberguerre

. le temps (2012) "Flame :le virus informatif le plus puissant au monde-"
.diffusion 29 mai 2012.
https://www.letemps.ch/no-section/flame-virus-informatique-plus-puissant-monde

"Y aura –t–il une cyberguerre froide entre les Etats Units et la Russie –"
. .RMC(2016).modifié le 16 décembre 2016
RMC.bFmtv.com/emission/y-aura-t-il-unecyber-guerrefroide-entre-lesétats-unis-et-la-russie-1072089.html.

« Piratage russe riposte US : la guerre numérique froide a -
commencé ».Ouest France(2016).modified 16 décembre2016
https://www.ouest-france.fr/monde/piratage-russe-riposte-us-la-guerre-froide-numerique-commence-468517

:Encyclopédies

wikipedia(2018), dernière ." Militarisme -"
modification le 13 juin 2018 ,
https://fr.wikipedia.org/wiki/Militarisme

wikipédia(2018).modifié le 02 juin 2018."La cyberguerre " -
https://fr.wikipedia.org/wiki/Cyberguerre

قائمة المراجع باللغة الانجليزية:

- Clarke, Richard A and. Knake ,Robert K. cyber war :Harper Collins e-Book,2010
http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20

List of cyber- weapons developed by the Pentagon to " .Ellen Nakashima,-
(diffusion may 31 .Washington Post(2011)."streamline computer warfare
.)2011

https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html?utm_term=.080fd

) (2004 softpower". mye,Joseph ."– Ny
https://www.belfercenter.org/sites/default/files/legacy/files/joe_nye_wielding_soft_power.pdf

The MIT Press . "Cyberpolitics in International Relations" . Choukri, Nazli -
Massachusetts(2012): England London .Cambridge
https://flavioufabc.files.wordpress.com/2017/02/cyberpolitics-and-international-relations.pdf

Poindexter, Dennis F.-
. copyrited " "the new cyberwar :technology and redifinition of Warfare
Material(2013).
https://www.amazon.com/New-Cyberwar-Technology-Redefinition-Warfare/dp/0786498439

(2016)" The CNAorporation [US] – "
https://www.cna.org/cna–Files/pdf/dop–2016–4–014231–1rev,pdf.

from cold war to cyberwar :the future of US- Russia "Fazio ,Federeca . -
Aspenia(2016). 21 décembre2016 . . "relations
https://www.aspeninstitute.it/aspenia-online/article/cold-war-cyber-war-future-us-russia-relations

"Chechnya ,Russia and 20 years of conflict"Mirovalev, Mansur. -
Newsgrid(2014).diffusion le11décembre2014
https://www.aljazeera.com/indepth/features/2014/12/chechnya-russia-20-years-conflict-20141211613105805 23.html

.BBC " haw cyber attak transformed Estonia"McGuinness,Damien . -
News(2017).modified April 27, 2017.
https://www.bbc.com/news/39655415

what's Ukraine doing to combat Russian cyber "Miller,Christopher . -
. Radio Liberty(2018). modified march "warefare ? Not enough
07,2018
https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html

:

- "شاهد كيف حدث التدخل الروسي المزعوم في الإنتخابات الأمريكية" . CNN (2018). آخر تحديث18 فيفري 2018

https:/arabiccnncom/world /wd–uselections–meddling–how–russia–did–it

فهرس المحتويات

المحتويات: